

Annals of Computer Science and Information Systems
Volume 12

**Position Papers of the 2017 Federated
Conference on Computer Science and
Information Systems**

September 3–6, 2017. Prague, Czech Republic



Maria Ganzha, Leszek Maciaszek, Marcin Paprzycki (eds.)



Annals of Computer Science and Information Systems, Volume 12

Series editors:

Maria Ganzha,

Systems Research Institute Polish Academy of Sciences and Warsaw University of Technology, Poland

Leszek Maciaszek,

Wrocław University of Economy, Poland and Macquarie University, Australia

Marcin Paprzycki,

Systems Research Institute Polish Academy of Sciences and Management Academy, Poland

Senior Editorial Board:

Wil van der Aalst,

Department of Mathematics & Computer Science, Technische Universiteit Eindhoven (TU/e), Eindhoven, Netherlands

Frederik Ahlemann,

University of Duisburg-Essen, Germany

Marco Aiello,

Faculty of Mathematics and Natural Sciences, Distributed Systems, University of Groningen, Groningen, Netherlands

Mohammed Atiquzzaman,

School of Computer Science, University of Oklahoma, Norman, USA

Barrett Bryant,

Department of Computer Science and Engineering, University of North Texas, Denton, USA

Ana Fred,

Department of Electrical and Computer Engineering, Instituto Superior Técnico (IST—Technical University of Lisbon), Lisbon, Portugal

Janusz Górski,

Department of Software Engineering, Gdansk University of Technology, Gdansk, Poland

Mike Hinchey,

Lero—the Irish Software Engineering Research Centre, University of Limerick, Ireland

Janusz Kacprzyk,

Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland

Irwin King,

The Chinese University of Hong Kong, Hong Kong

Juliusz L. Kulikowski,

Natęcz Institute of Biocybernetics and Biomedical Engineering, Polish Academy of Sciences, Warsaw, Poland

Michael Luck,

Department of Informatics, King's College London, London, United Kingdom

Jan Madey,

Faculty of Mathematics, Informatics and Mechanics at the University of Warsaw, Poland

Stan Matwin,

Dalhousie University, University of Ottawa, Canada and Institute of Computer Science, Polish Academy of Science, Poland

Michael Segal,

Ben-Gurion University of the Negev, Israel

Andrzej Skowron,

Faculty of Mathematics, Informatics and Mechanics at the University of Warsaw, Poland

John F. Sowa,

VivoMind Research, LLC, USA

Editorial Associate:

Katarzyna Wasielewska,

Systems Research Institute Polish Academy of Sciences, Poland

Paweł Sitek,

Kielce University of Technology, Kielce, Poland

T_EXnical editor: Aleksander Denisiuk,

University of Warmia and Mazury in Olsztyn, Poland

Position Papers of the 2017 Federated Conference on Computer Science and Information Systems

Maria Ganzha, Leszek Maciaszek, Marcin Paprzycki
(eds.)



2017, Warszawa,
Polskie Towarzystwo
Informatyczne

Annals of Computer Science and Information Systems, Volume 12
Position Papers of the 2017 Federated Conference on Computer Science
and Information Systems

USB: ISBN 978-83-922646-1-3

WEB: ISBN 978-83-922646-0-6

ISSN 2300-5963

DOI 10.15439/978-83-922646-0-6

© 2017, Polskie Towarzystwo Informatyczne

Ul. Solec 38/103

00-394 Warsaw

Poland

Contact: secretariat@fedcsis.org

<http://annals-csis.org/>

Cover photo:

Konrad Kosacz,

Elbląg, Poland

Also in this series:

Volume 13: Communication Papers of the 2017 Federated Conference on Computer Science and Information Systems, **ISBN WEB: 978-83-922646-2-0, ISBN USB: 978-83-922646-3-7**

Volume 11: Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, **ISBN WEB: 978-83-946253-7-5, ISBN USB: 978-83-946253-8-2,**

ISBN ART: 978-83-946253-9-9

Volume 10: Proceedings of the Second International Conference on Research in Intelligent and Computing in Engineering, **ISBN WEB: 978-83-65750-05-1,**

ISBN USB: 978-83-65750-06-8

Volume 9: Position Papers of the 2016 Federated Conference on Computer Science and Information Systems, **ISBN WEB: 978-83-60810-93-4, ISBN USB: 978-83-60810-94-1**

Volume 8: Proceedings of the 2016 Federated Conference on Computer Science and Information Systems, **ISBN WEB: 978-83-60810-90-3, ISBN USB: 978-83-60810-91-0,**

ISBN ART: 978-83-60910-92-7

Volume 7: Proceedings of the LQMR Workshop, **ISBN WEB: 978-83-60810-78-1,**

ISBN USB: 978-83-60810-79-8

Volume 6: Position Papers of the 2015 Federated Conference on Computer Science and Information Systems, **ISBN WEB: 978-83-60810-76-7, ISBN USB: 978-83-60810-77-4**

Volume 5: Proceedings of the 2015 Federated Conference on Computer Science and Information Systems, **ISBN WEB: 978-83-60810-66-8, ISBN USB: 978-83-60810-67-5**

Volume 4: Proceedings of the E2LP Workshop, **ISBN WEB: 978-83-60810-64-4,**

ISBN USB: 978-83-60810-63-7

Volume 3: Position Papers of the 2014 Federated Conference on Computer Science and Information Systems, **ISBN WEB: 978-83-60810-60-6, ISBN USB: 978-83-60810-59-0**

Volume 2: Proceedings of the 2014 Federated Conference on Computer Science and Information Systems, **WEB: ISBN 978-83-60810-58-3, USB: ISBN 978-83-60810-57-6,**

ART: ISBN 978-83-60810-61-3

Volume 1: Position Papers of the 2013 Federated Conference on Computer Science and Information Systems (FedCSIS), **ISBN WEB: 978-83-60810-55-2, ISBN USB: 978-83-60810-56-9**

DEAR Reader, it is our pleasure to present to you Position Papers of the 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), which took place, for the first time outside of Poland, in Prague, Czech Republic, on September 3-6, 2017.

We consider position papers to be important enough to recognize them as a separate publication. As you will see, they comprise two categories of contributions – *challenge papers* and *emerging research papers*. *Challenge papers* propose and describe research challenges in theory, or practice, of computer science and information systems. Papers in this category are based on deep understanding of existing research or industrial problems. Based on such understanding and experience, they define new exciting research directions and show why these directions are crucial to the society at large. *Emerging research papers* present preliminary research results from work-in-progress based on sound scientific approach but presenting work not completely validated as yet. They describe precisely the research problem and its rationale. They also define precisely the intended future work including the expected benefits from solution to the tackled problem. Subsequently, they may be more conceptual than experimental.

FedCSIS 2017 was Chaired by prof. Pavel Tvrdik, while prof. Jan Janousek acted as the Chair of the Organizing Committee. This year, FedCSIS was organized by the Polish Information Processing Society (Mazovia Chapter), IEEE Poland Section Computer Society Chapter, Systems Research Institute Polish Academy of Sciences, Warsaw University of Technology, Wrocław University of Economics, and Czech Technical University in Prague.

FedCSIS 2017 was technically co-sponsored by: IEEE Region 8, IEEE Czechoslovakia Section, IEEE Poland Section, IEEE Computer Society, IEEE Computer Society Technical Committee on Intelligent Informatics, IEEE Czechoslovakia Section Computer Society Chapter, IEEE Poland Section Gdańsk Computer Society Chapter Poland, SMC Technical Committee on Computational Collective Intelligence, IEEE Poland Section Systems, Man, and Cybernetics Society Chapter, IEEE Poland Section Control System Society Chapter, IEEE Poland Section Computational Intelligence Society Chapter, ACM Special Interest Group on Applied Computing, Łódź ACM Chapter, International Federation for Information Processing, Committee of Computer Science of the Polish Academy of Sciences, Polish Operational and Systems Research Society, Mazovia Cluster ICT Poland, Polski Klaster Badań i Rozwoju Internetu Rzeczy, and Eastern Cluster ICT Poland. FedCSIS 2017 was sponsored by Intel, Profinit and Abra.

FedCSIS 2017 consisted of the following events (conferences, symposia, workshops, special sessions). These events were grouped into FedCSIS conference areas, of various degree of integration. Specifically, those listed without indication of the year 2017 signify "abstract areas" with no direct paper submissions to them (but with submissions to their enclosed events).

- **AAIA'17 – 12th International Symposium Advances in Artificial Intelligence and Applications**
 - AIMA'17 – 7th International Workshop on Artificial Intelligence in Medical Applications

- AIRIM'17 – 2nd International Workshop on AI aspects of Reasoning, Information, and Memory
- ASIR'17 – 7th International Workshop on Advances in Semantic Information Retrieval
- JAWS'17 – 11th Joint Agent-oriented Workshops in Synergy
- LTA'17 – 2st International Workshop on Language Technologies and Applications
- WCO'17 – 10th International Workshop on Computational Optimization
- **CSS - Computer Science & Systems**
 - CANA'17 – 10th Computer Aspects of Numerical Algorithms
 - C&SS'17 – 4th International Conference on Cryptography and Security Systems
 - CPORA'17 – 2nd Workshop on Constraint Programming and Operation Research Applications
 - MMAP'17 – 10th International Symposium on Multimedia Applications and Processing
 - WAPL'17 – 6th Workshop on Advances in Programming Languages
 - WSC'17 – 9th Workshop on Scalable Computing
- **iNetSApp – International Conference on Innovative Network Systems and Applications**
 - INSERT'17 – 1st International Conference on Security, Privacy, and Trust
 - IoT-ECAW'17 – 1st Workshop on Internet of Things – Enablers, Challenges and Applications
 - WSN'17 – 6th International Conference on Wireless Sensor Networks
- **IT4MBS – Information Technology for Management, Business & Society**
 - AITM'17 – 15th Conference on Advanced Information Technologies for Management
 - ISM'17 – 12th Conference on Information Systems Management
 - IT4L'17 – 5th Workshop on Information Technologies for Logistics
 - KAM'17 – 23rd Conference on Knowledge Acquisition and Management
- **SSD&A – Software Systems Development & Applications**
 - IWCPs'17 – 4th International Workshop on Cyber-Physical Systems
 - LASD'17 – 1st International Conference on Lean and Agile Software Development
 - MIDI'17 – 4th Conference on Multimedia, Interaction, Design and Innovation
 - SEW-37 – The 37th IEEE Software Engineering Workshop

- **DS-RAIT'17 – 4th Doctoral Symposium on Recent Advances in Information Technology**

Each paper, found in this volume, was refereed by at least two referees.

The program of FedCSIS required a dedicated effort of many people. Each event constituting FedCSIS had its own Organizing and Program Committee. We would like to express our warmest gratitude to all Committee members for their hard work in attracting and later refereeing 497 regular submissions.

We thank the authors of papers for their great contribution to research and practice in computing and information systems. We thank the invited speakers for sharing their knowledge and wisdom with the participants. Finally, we thank all those responsible for staging the conference in Prague. Organizing a conference of this scope and level could only be achieved by the collaborative effort of a highly capable team taking charge of such matters as conference registration sys-

tem, finances, the venue, social events, catering, handling all sorts of individual requests from the authors, preparing the conference rooms, etc.

We hope you had an inspiring conference and an unforgettable stay in the beautiful city of Prague. We hope to meet you again for FedCSIS 2018 in Poznań, Poland.

Co-Chairs of the FedCSIS Conference Series

Maria Ganzha, Warsaw University of Technology, Poland and Systems Research Institute Polish Academy of Sciences, Warsaw, Poland

Leszek Maciaszek, Wrocław University of Economics, Wrocław, Poland and Macquarie University, Sydney, Australia

Marcin Paprzycki, Systems Research Institute Polish Academy of Sciences, Warsaw Poland and Management Academy, Warsaw, Poland

Annals of Computer Science and Information Systems,
Volume 12

Position Papers of the 2017 Federated
Conference on Computer Science and
Information Systems (FedCSIS)

September 3–6, 2017. Prague, Czech Republic

TABLE OF CONTENTS

**12TH INTERNATIONAL SYMPOSIUM ADVANCES IN ARTIFICIAL
INTELLIGENCE AND APPLICATIONS**

Call For Papers	1
How effective is Transfer Learning method for image classification <i>Marek Dąbrowski, Tomasz Michalik</i>	3
Topological structures as a tool for formal modelling of rough sets <i>Adam Grabowski, Roland Coghetto</i>	11
Direct Potentiality Assimilation for Improving Multi-Layered Neural Networks <i>Ryotaro Kamimura</i>	19
Concepts Ontology Algebras and Role Descriptions <i>Cyrus F. Nourani, Patrik Eklund</i>	25
Rough Sets for Trees of Executions <i>Krzysztof Pancierz</i>	33
Evaluation of classifiers: current methods and future research directions <i>Katarzyna Stapor</i>	37

**7TH INTERNATIONAL WORKSHOP ON ARTIFICIAL INTELLIGENCE IN
MEDICAL APPLICATIONS**

Call For Papers	41
A Deep Learning-Based Approach for the Recognition of Sleep Disorders in Patients with Cognitive Diseases: A Case Study <i>Giovanni Paragliola, Antonio Coronato</i>	43

**7TH INTERNATIONAL WORKSHOP ON ADVANCES IN SEMANTIC
INFORMATION RETRIEVAL**

Call For Papers	49
FLOODS: A Succinct File System Structure <i>Daniel Peters, Johannes Fischer, Florian Thiel, Jean-Pierre Seifert</i>	51

11TH JOINT AGENT-ORIENTED WORKSHOPS IN SYNERGY

Call For Papers	59
On local minima in distributed energy scheduling <i>Astrid Nieße, Joerg Bremer, Sebastian Lehnhoff</i>	61

<hr/>	
2ND INTERNATIONAL WORKSHOP ON LANGUAGE TECHNOLOGIES AND APPLICATIONS	
Call For Papers	69
A Web Corpus for eCare: Collection, Lay Annotation and Learning -First Results- <i>Marina Santini, Arne Jönsson, Mikael Nyström, Marjan Alirezai</i>	71
<hr/>	
10TH INTERNATIONAL WORKSHOP ON COMPUTATIONAL OPTIMIZATION	
Call For Papers	79
On Pathological Fitness Landscapes for Constrained Combinatorial Optimization <i>Gary Greenfield, Aldeida Aleti</i>	81
<hr/>	
COMPUTER SCIENCE & SYSTEMS	
Call For Papers	87
<hr/>	
2ND WORKSHOP ON CONSTRAINT PROGRAMMING AND OPERATION RESEARCH APPLICATIONS	
Call For Papers	89
An example of the satisfiability problem in the continuous structure <i>Marek Balcer</i>	91
<hr/>	
6TH WORKSHOP ON ADVANCES IN PROGRAMMING LANGUAGES	
Call For Papers	95
Welltype: Language elements for multiparadigm programming <i>Áron Baráth, Zoltán Porkoláb</i>	97
<hr/>	
INTERNATIONAL CONFERENCE ON INNOVATIVE NETWORK SYSTEMS AND APPLICATIONS	
Call For Papers	103
<hr/>	
1ST INTERNATIONAL CONFERENCE ON SECURITY, PRIVACY, AND TRUST	
Call For Papers	105
Risk Management in Access Control Policies <i>Pierrette Annie Evina, Faten Labenne Ayachi, Faouzi Jaidi</i>	107
Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection <i>Artur Rot, Boguslaw Olszewski</i>	113
A Modular Testbed for Intelligent Meters and their Ecosystem <i>Jan Wetzlich, Martin Nischwitz, Florian Thiel, Jean-Pierre Seifert</i>	119
<hr/>	
1ST WORKSHOP ON INTERNET OF THINGS - ENABLERS, CHALLENGES AND APPLICATIONS	
Call For Papers	127
Assessment of Feasible Methods Used by the Health Care Industry for Real Time Location <i>Jay Pancham, Richard Millham, Simon Fong</i>	129
CHARIOT: An IoT Middleware for the Integration of Heterogeneous Entities in a Smart Urban Factory <i>Cem Akpolat, Doruk Sahinel, Fikret Sivrikaya, Grzegorz Lehmann, Sahin Albayrak</i>	135

<hr/>	
6TH INTERNATIONAL CONFERENCE ON WIRELESS SENSOR NETWORKS	
Call For Papers	143
Analysis of the new modulation and coding techniques for VDSL <i>Tomáš Pajda, Rastislav Roka</i>	145
<hr/>	
INFORMATION TECHNOLOGY FOR MANAGEMENT, BUSINESS & SOCIETY	
Call For Papers	149
<hr/>	
15TH CONFERENCE ON ADVANCED INFORMATION TECHNOLOGIES FOR MANAGEMENT	
Call For Papers	151
Identification of Business Relevant Features in Information Systems <i>Jiri Matula, Jaroslav Zacek</i>	153
Temporal Evaluation of Business Processes Using Timed Colored Petri Nets <i>Yoshiyuki Shinkawa, Ryoya Shiraki</i>	161
<hr/>	
23RD CONFERENCE ON KNOWLEDGE ACQUISITION AND MANAGEMENT	
Call For Papers	169
Information Quality Challenges for the Preservation of Norwegian Public Sector Records <i>Markus Helfert, Petter Reinholdtsen, Thomas Sødning</i>	171
Knowledge Management in the Cloud Computing Model - Challenges, Opportunities and Risks <i>Artur Rot, Małgorzata Sobińska</i>	177
<hr/>	
SOFTWARE SYSTEMS DEVELOPMENT & APPLICATIONS	
Call For Papers	183
<hr/>	
4TH INTERNATIONAL WORKSHOP ON CYBER-PHYSICAL SYSTEMS	
Call For Papers	185
Industrial Use Cases of Cyber Physical Systems in EU Projects: Preliminary Study <i>Rima Al-Ali</i>	187
Utilising Latent Data in Smart Buildings: A Process Model to Collect, Analyse and Make Building Data Accessible for Smart Industries <i>Zohreh Pourzolfaghar, Markus Helfert</i>	195
<hr/>	
4TH DOCTORAL SYMPOSIUM ON RECENT ADVANCES IN INFORMATION TECHNOLOGY	
Call For Papers	203
Virtual Tour for Smart Home Developed in Unity Engine and Connected with Arduino <i>Erik Kučera, Erich Stark, Oto Haffner</i>	205

12th International Symposium Advances in Artificial Intelligence and Applications

A AIA'17 will bring scientists, developers, practitioners, and users to present their latest research, results, and ideas in all areas of Artificial Intelligence. We hope that successful applications presented at AAIA'17 will be of interest to researchers who want to know about both theoretical advances and latest applied developments in AI.

TOPICS

Papers related to theories, methodologies, and applications in science and technology in this theme are especially solicited. Topics covering industrial applications and academic research are included, but not limited to:

- Decision Support
- Machine Learning
- Fuzzy Sets and Soft Computing
- Rough Sets and Approximate Reasoning
- Data Mining and Knowledge Discovery
- Data Modeling and Feature Engineering
- Data Integration and Information Fusion
- Hybrid and Hierarchical Intelligent Systems
- Neural Networks and Deep Learning
- Bayesian Networks and Bayesian Reasoning
- Case-based Reasoning and Similarity
- Web Mining and Social Networks
- Business Intelligence and Online Analytics
- Robotics and Cyber-Physical Systems
- AI-centered Systems and Large-Scale Applications

We also encourage researchers interested in the following topics to submit papers directly to the corresponding workshops, which are integral parts of AAIA'17:

- AI in Computational Optimization (WCO'17 workshop)
- AI in Language Technologies (LTA'17 workshop)
- AI in Medical Applications (see AIMA'17 workshop)
- AI in Reasoning and Computational Foundations (AIRIM'17 workshop)
- AI in Information Retrieval (ASIR'17 workshop)

All papers accepted to the main track of AAIA'17 and to the above workshops will be treated equally in the conference programme and will be equally considered for the awards listed below.

PROFESSOR ZDZISLAW PAWLAK BEST PAPER AWARDS

We are proud to continue the tradition started during the AAIA'06 and award two "Professor Zdzislaw Pawlak Best Paper Awards" for contributions which are outstanding in their scientific quality. The two award categories are:

- Best Student Paper—papers qualifying for this award must be marked as "Student full paper" to be eligible.
- Best Paper Award.

In addition to a certificate, each award carries a prize of 300 EUR provided by the Mazowsze Chapter of the Polish Information Processing Society.

ZDZISLAW PAWLAK AWARD COMMITTEE

- **Kacprzyk, Janusz**, Polish Academy of Sciences, Poland
- **Kwaśnicka, Halina**, Wrocław University of Technology, Poland
- **Marek, Victor**, University of Kentucky, United States
- **Markowska-Kaczmar, Urszula**, Wrocław University of Technology, Poland
- **Matwin, Stan**, Dalhousie University, Canada
- **Michalewicz, Zbigniew**, University of Adelaide, Australia
- **Skowron, Andrzej**, University of Warsaw, Poland
- **Śluzek, Andrzej**, Khalifa University, United Arab Emirates

SECTION EDITORS

- **Janusz, Andrzej**, University of Warsaw, Poland
- **Śluzek, Dominik**, University of Warsaw, Poland

REVIEWERS

- **Bartkowiak, Anna**, Wrocław University, Poland
- **Bazan, Jan**, University of Rzeszów, Poland
- **Betlinski, Pawel**, Security On Demand, Poland
- **Borkowski, Janusz**, Polish-Japanese Academy of Information Technology & Security On Demand, Poland
- **Błaszczyszński, Jerzy**, Poznań University of Technology, Poland
- **Carrizosa, Emilio**, Universidad de Sevilla, Spain
- **Chakraverty, Shampa**, Netaji Subhas Institute of Technology, India
- **do Carmo Nicoletti, Maria**, UFSCar & FACCAMP, Brazil
- **Duentsch, Ivo**, Brock University, Canada
- **Eklund, Patrik**, Umeå University, Sweden
- **Foresti, Gian Luca**, University of Udine, Italy
- **Froelich, Wojciech**, University of Silesia, Poland
- **Girardi, Rosario**, Federal University of Maranhão, Brazil
- **Jaromczyk, Jerzy**, University of Kentucky, United States
- **Jatowt, Adam**, Kyoto University, Japan

- **Jin, Xiaolong**, Institute of Computing Technology, Chinese Academy of Sciences, China
- **Karhang, Maylor Leung**, Universiti Tunku Abdul Rahman, Malaysia
- **Kasprzak, Włodzimierz**, Warsaw University of Technology, Poland
- **Kayakutlu, Gulgun**, Istanbul Technical University, Turkey
- **Konikowska, Beata**, Polish Academy of Sciences, Poland
- **Korbicz, Józef**, University of Zielona Góra, Poland
- **Kostek, Bożena**, Gdańsk University of Technology, Poland
- **Kryszkiewicz, Marzena**, Warsaw University of Technology, Poland
- **Kulikowski, Juliusz**, Institute of Biocybernetics and Biomedical Engineering, Poland
- **Lopes, Lucelene**, PUCRS, Brazil
- **Madalińska-Bugaj, Ewa**, University of Warsaw, Poland
- **Matson, Eric T.**, Purdue University, United States
- **Menasalvas, Ernestina**, Universidad Politécnica de Madrid, Spain
- **Miyamoto, Sadaaki**, University of Tsukuba, Japan
- **Moshkov, Mikhail**, King Abdullah University of Science and Technology, Saudi Arabia
- **Myszkowski, Paweł B.**, Wrocław University of Technology, Poland
- **Nourani, Cyrus F.**, Akdmkrd-DAI TU Berlin & Munich Transmedia & SFU Burnaby, Germany
- **Nowostawski, Mariusz**, Norwegian University of Technology and Science (NTNU), Norway
- **Ogiela, Marek**, AGH University of Science and Technology, Poland
- **Ohsawa, Yukio**, University of Tokyo, Japan
- **Peters, Georg**, Munich University of Applied Sciences, Germany
- **Po, Laura**, Università di Modena e Reggio Emilia, Italy
- **Porta, Marco**, University of Pavia, Italy
- **Przybyła-Kasperek, Małgorzata**, University of Silesia, Poland
- **Raghavan, Vijay**, University of Louisiana at Lafayette, United States
- **Rakus-Andersson, Elisabeth**, Blekinge Institute of Technology, Sweden
- **Ramanna, Sheela**, University of Winnipeg, Canada
- **Ras, Zbigniew**, University of North Carolina at Charlotte, United States
- **Rauch, Jan**, University of Economics, Prague, Czech Republic
- **Reformat, Marek**, University of Alberta, Canada
- **Ruta, Dymitr**, EBTC, Khalifa University of Science and Technology, United Arab Emirates
- **Schaefer, Gerald**, Loughborough University, United Kingdom
- **Sikora, Marek**, Silesian University of Technology, Poland
- **Sikos, Leslie F.**, Flinders University, Australia
- **Subbotin, Sergey**, Zaporizhzhya National Technical University, Ukraine
- **Sydow, Marcin**, Polish Academy of Sciences & Polish-Japanese Academy of Information Technology, Poland
- **Szczęch, Izabela**, Poznań University of Technology, Poland
- **Szczuka, Marcin**, University of Warsaw, Poland
- **Szpakowicz, Stan**, University of Ottawa, Canada
- **Szwed, Piotr**, AGH University of Science and Technology, Poland
- **Tomczyk, Arkadiusz**, Lodz University of Technology, Poland
- **Unland, Rainer**, Universität Duisburg-Essen, Germany
- **Unold, Olgierd**, Wrocław University of Technology, Poland
- **Velastin, Sergio A.**, Kingston University, United Kingdom
- **Weber, Richard**, Universidad de Chile, Chile
- **Werghe, Naoufel**, Khalifa University of Science and Technology, United Arab Emirates
- **Zakrzewska, Danuta**, Łódź University of Technology, Poland
- **Zielosko, Beata**, University of Silesia, Poland
- **Ziółko, Bartosz**, AGH University of Science and Technology, Poland

How effective is Transfer Learning method for image classification

Marek Dąbrowski,
 Tomasz Michalik
 Orange Polska, Centrum
 Badawczo-Rozwojowe, ul.
 Obrzeźna 7, 02-691 Warszawa
 Email: {marek.dabrowski,
 tomasz.michalik}@orange.com

Abstract—This paper deals with re-training neural network-based image classification model, using so-called Transfer Learning approach. This method allows for creating a new image classifier, reusing pre-trained weights from a publicly available model. Our study gives some insight on accuracy of re-trained models and provides guidelines concerning required number of training examples. Presented results may be useful for computer vision practitioners, who would like to adapt results of state-of-the-art research on neural networks for their own customized image recognition models.

I. INTRODUCTION

MACHINE learning and neural networks dominate in recent research on computer vision. Deep learning and convolutional neural networks [1][2] proved to be especially successful in solving various computer vision problems, including image classification, segmentation, object detection etc.

The goal of image classification is to guess the object presented in the picture, from a set of pre-defined labels, or classes. Convolutional neural networks have been used for image classification since pioneering research by Yann LeCun in 1980ies [3]. More recently, since the work of A. Krizhevsky [4] the same basic concepts are applied to classification of colorful images (photos).

The general idea of deep neural network for image classification is depicted in Fig.1. Input data consists of numerical values for RGB color intensities of image pixels. The input is processed by artificial neural units, structured in multiple interconnected layers. The internal units may be of different types: convolutional, pooling and fully-connected, usually intervened with each other according to some complicated model architecture. The last layer is the classification layer, which calculates output probabilities. In the case of image classification problem, these probabilities represent likelihood that the image belongs to given pre-defined class. For example, the output layer may calculate likelihood that the input image depicts a “cat”, or a “dog”, and so on.

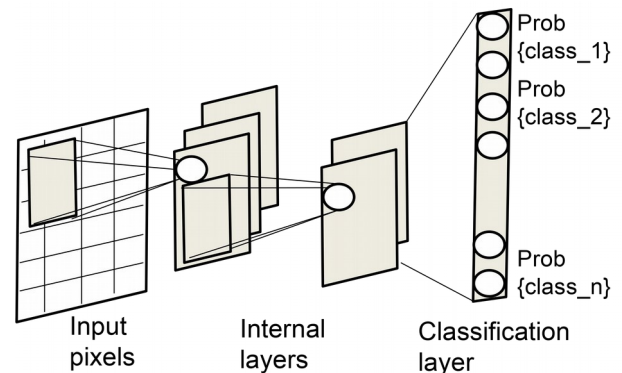


Fig. 1 Illustration of multi-layer convolutional model for image classification

Recent progress in research on image recognition has been enabled, among others, by increased availability of high quality training data. The Imagenet repository [5] is freely available for research and contains about 14 million human-annotated images, grouped in 21 thousand classes. In an annual contest organized by Imagenet, researchers compete to achieve best results in typical computer vision problems. For the purpose of this contest, 1000 classes have been specially selected, corresponding to a wide overview of objects that may typically occur in real-life images. These 1000 classes (each with about 1000 training images) constitute a special “Imagenet1000” corpus, which is often treated in research [6].

It is not uncommon for top research teams to publish publicly not only the research results, but also pre-trained models of neural networks that have been successful in Imagenet contest. These publicly available pre-trained models can be freely used for research and even commercial purposes. Notable example is the “GoogleNet” model (see Fig.2) proposed by Google in 2014 [7][8][9], improved in consecutive years, and made publicly available together with open source computation toolkit Tensorflow [10].

Our research on image classification has been motivated by a concept of photo album service for home users, where submitted photos would be automatically tagged with semantic information about depicted objects.

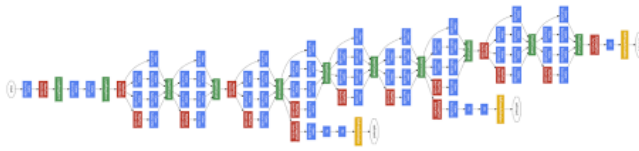


Fig. 2 “GoogleNet”: state-of-the-art multi-layer convolutional model for image classification

The simplest way to implement such service is to use open source computation framework, with standard publicly available image classification model pre-trained on Imagenet1000 corpus. Such model would categorize among various kinds of standardized categories, which include among others a type of place where photo was taken (e.g. “lighthouse”, “shop”), type of depicted animal (“Egyptian cat”, “English foxhound”), or type of clothing (“T-shirt”, “blue jeans”). Such approach has some disadvantages for practical deployment. On one hand, the “one-size-fits-all” approach is too generic if the foreseen service should focus on one particular applicative area, e.g. to recognize only geographical places, or types of animals. On the other hand, the Imagenet1000 categories are over-specified in some selected fields, like for example they contain 120 dog breeds to recognize among. Such level of detail is usually not necessary.

Thus, aiming to build a specific service based on image recognition technology, we would rather create our own custom image classifier. This paper focuses on methods how we can do that with minimum effort.

II. TRANSFER LEARNING

It is known that training image classification from scratch is a very long and difficult process and may take weeks to complete on high-performance hardware [7]. Thus, a Transfer Learning method is often proposed to simplify it [12]. It assumes that a new classification layer is learned, while all weights of internal layers (remind that for example the GoogleNet model has 22 of them) are transferred from a pre-trained model. The process for practical usage of Transfer Learning is the following:

1. Get a previously trained model, e.g. from [11].
2. Split the old model architecture into two parts:
 - a. All hidden layers of the neural network, with their structure (connections) and previously learned weights, will be copied into the new model.
 - b. The last layer of neural network, which performs actual classification into one of the classes, is strictly related with the old model and will be disregarded in the new model.
3. Prepare a new set of training examples (images labelled with appropriate class name, as required for the new model).
4. For a new set of training images, calculate the output values after passing through the first part of neural

network (the one that is transferred into the new model). The numerical value calculated as output of next-to-last layer of original model for a given image, will be called a “bottleneck”.

5. Add a new final fully-connected layer, which will now constitute the last layer of new neural network model. This new final layer will calculate the probability of given image belonging to a given class.
6. Train the new final layer with previously calculated “bottlenecks” as input, and a set of new “ground truth” labels that denote true classes of training images.

Thanks to that method, we can create a new image classification model with our own classes and labels, within several hours instead of weeks, on standard hardware.

An example neural network architecture with new re-trained classifier is presented in Fig.3. Remark that the new classifier may contain some classes that overlap with the old classifier (we will call them “*internal*” classes, shortly INT) and some classes that are totally new (“*external*” classes, EXT). Only in the case of EXT classes we can truly claim using the Transfer Learning method, since the training images belonging to them have not been previously used for training internal weights of deep neural network. In the case of INT classes, their training images may have been previously used in training the internal features, so we cannot really speak of Transfer Learning. However, the INT classes will be discussed in our experiments since in practice they may be equally useful in creating a service-oriented custom classifier.

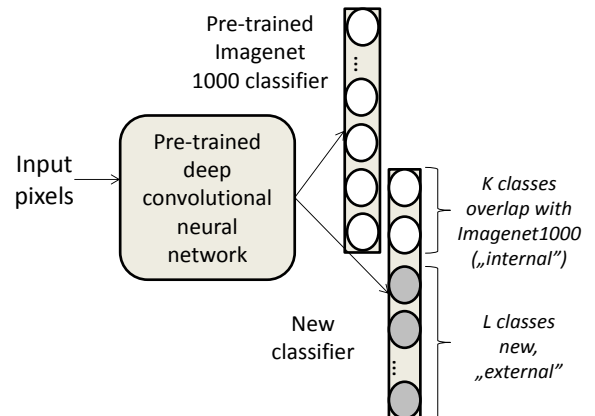


Fig. 3. Transfer learning setup: new classifier on top of pre-trained deep convolutional network

Fig.4 gives additional explanation of the distinction between “*external*” and “*internal*” classes. The left column is an example excerpt from list of class labels in standard Imagenet1000 model. The right column presents a fictional classifier with 6 custom classes, among which 3 overlap with Imagenet1000 (INT) and 3 are outside of the Imagenet1000 set (EXT).

No	Imagenet1000 classifier	Custom classifier with 6 classes
1	Bakery	Bakery (INT)
2	Barn	Barn (INT)
3	Lighthouse	Lighthouse (INT)
4	Electric ray	Embankment (EXT)
5	English foxhound	Embassy (EXT)
6	English setter	Farm building (EXT)
7	Eggnog	
8	Egyptian cat	
...	...	

Fig. 4. Example fictional custom classifier with 6 classes. The 3 INT classes in custom classifier are the same as Imagenet1000 model, while 3 EXT classes are new.

The Transfer Learning method has been previously studied in scientific literature, e.g. in [12] and its practical usage is not an original idea. The software scripts for modifying the standard Imagenet1000 model are available with popular neural network computation frameworks, like Tensorflow [11]. In previous work [13] we have studied the Transfer Learning method, focusing on practical guidelines for setting hyperparameters of re-training process, as well as evaluation of re-training speed on several typical hardware platforms. What we found missing in the literature is, however, a comprehensive evaluation of performance of re-trained models. In this paper we would like to share our experience in this regard, in particular trying to answer the following questions:

- What accuracy we can expect from re-trained model? We know that the publicly available GoogleNet model for Imagenet1000 classification can achieve about 80% accuracy (meaning that it gives correct result on 80% of test images). We can expect that the re-trained model could be less accurate, since the internal features were effectively trained on different set of images than the final classifier. But how can we quantify the loss of accuracy?
- How many training examples do we actually need in re-trained classes to achieve acceptable accuracy of end-user service?

III. ACCURACY OF RETRAINED MODEL

First goal of our research was to assess accuracy of a re-trained image recognition model. For our experiments we have used Tensorflow [10], open source software library from Google. It performs machine learning computations, including neural network models, on various types of hardware, with CPU and GPU. Tensorflow implements the Transfer Learning method, with “GoogleNet” model as basis for re-training. We made our experiments on a typical desktop PC with 4 CPU cores and 8GB RAM, equipped with GPU card NVIDIA GeForce GTX 960.

As a target model for Transfer Learning we have defined a custom set of 100 classes, manually and arbitrarily selected

from wide Imagenet corpus, which has 21 thousand classes in total. For each new class we have verified if it is, or it is not, included in the standard Imagenet1000 model. Referring again to the example presented in Fig 4, the class “bakery” is included in Imagenet 1000 and the original GoogleNet model has been trained with examples belonging to this class. This class is thus considered “internal” (INT) class, in contrary to, for example, “embassy” which is a new class, named “external” (EXT).

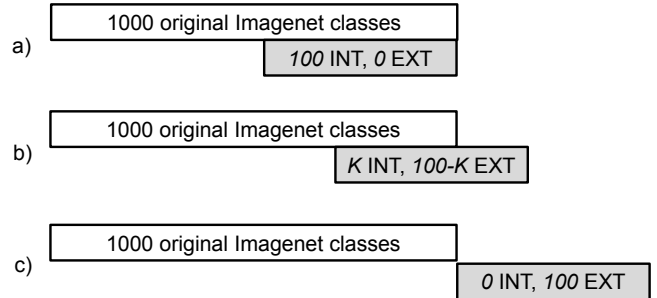


Fig. 5. Various mix of INT and EXT classes in the custom classifier with 100 classes: a) full overlap, b) partial overlap, c) no overlap

Depending on particular service scenario, the target custom classifier may contain certain number of INT and EXT classes. Thus, in our experiments we have varied the mix of their mutual proportions (see Fig.5).

Intuitively, we may expect that the INT classes may be more accurately recognized by the new re-trained classifier, since they are somehow “known” by the model from the beginning. On the other hand, we may expect that the EXT classes are less accurately recognized by the new classifier, since they were not taken into account in prior training process of internal layers. Thus, we were interested in studying how the overall accuracy depends on the mix of “new” (EXT) and “old” (INT) classes, which reflects somehow the level of similarity between the “old” and the “new” model.

We have used the re-training procedure as described in our previous work [13]. The classifier layer has been trained with Stochastic Gradient Descent algorithm [1], which takes the forward propagation loss (cross-entropy loss), calculates the gradients in backward propagation and then changes the weights of the model trying to minimize the loss. The learning rate value tells how fast the optimizer should converge to minimal loss. Based on [13], the chosen parameter setting was as follows: training steps=10000, the type of optimization algorithm was Adam Optimizer with learning rate $\alpha=0.01$ and epsilon=0.1 (a small constant for numerical stability), train batch size=100. For each re-trained class we have downloaded about 1000 training images from the Imagenet corpus.

The accuracy metric has been computed on a test set, created by putting-off 10% of images from the overall corpus. We have used two typical test metrics. *Top-1*

accuracy is defined as ratio of correct classification results in the entire test set (where correct result means: “the label with maximum score is equal to ground truth”). The *Top-5 accuracy* metric is less restrictive and defined as ratio of correct classification results in the test set, but the correct result is now: “the ground truth label is among 5 maximum-score labels assigned by the classification algorithm”.

We have evaluated separately the accuracy metrics for the sets of INT and EXT classes. In fact, we have measured “per-class” accuracy, that is a separate metric value for each of 100 classes in the re-trained model. Then, we define the “INT Top-1” accuracy as the average among all “internal” classes. Respectively, the “EXT Top-1” accuracy is defined as average accuracy among the “external” classes. As mentioned earlier, we expect EXT accuracy to be lower than INT accuracy, since it covers classes that had not been known in prior pre-training process.

To mitigate impact of arbitrary choice of set of target classes, we have repeated each experiment (i.e. performed re-training and measured resulting accuracy) five times, assuming different set of target classes, while keeping the same proportion of EXT and INT. The result is reported as an average with 5% confidence intervals.

Fig. 6 presents results of accuracy of re-trained models with different mix of EXT and INT classes. Starting from the left, “100% INT” means that all classes of the re-trained model overlapped with the original Imagenet1000. Then, we have gradually introduced more and more external classes. On the extreme right hand-side, all classes of the re-trained model are “new”, meaning that the scenario is a full Transfer Learning.

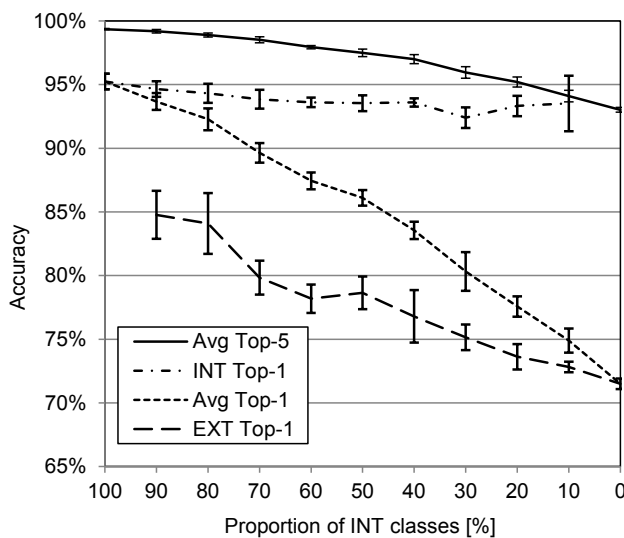


Fig. 6. Accuracy of re-trained 100-classes model with different proportions of INT and EXT classes

First, let us have a look at the “Avg Top-1” line in Fig.6. It depicts overall quality of the re-trained model, not knowing how different types of classes perform. So, in the

case of 100% internal classes, the Top-1 accuracy is about 95%, which is very high value (almost all images in test corpus are properly classified). Considering that all the classes overlap with the original Imagenet1000 model, we can say that re-training the classification layer does not degrade the performance (which is not so surprising since all the images used for re-training have been previously used to train the internal features of the model).

Going to the right, however, the accuracy drops, since more and more classes and training images are “new”, not used before for training the internal features. At the extreme case, where 100% classes are new, we note Top-1 accuracy of 71.5%, which means that about 3 in 4 test images are still properly recognized. The “Top-5” accuracy metric shows that this less restrictive metric drops from 99% to 93% in the Transfer Learning scenario.

A Top-1 accuracy drop from 95% to 71% is noticeable, but perhaps acceptable, taking into account the easiness and low computational cost of obtaining the re-trained model, comparing to training it from scratch.

The lines marked as “INT Top-1” and “EXT Top-1” give us a little more insight into performance of “old” and “new” classes separately. The “INT” classes that were present in original model and remained in the re-trained one, keep the over-90% accuracy. The internal features of original model were actually trained on them, so we could expect that re-training does not significantly impact these classes. For EXT classes, we observe that their Top-1 accuracy is between 85% and 71% throughout tested range of classes mix.

To confirm the outcome of that experiment, we have repeated it in a scenario with 200-classes classifier, instead of 100 classes. The results are depicted in Fig.7.

Since this experiment was just a confirmation of previous one, this time we did not repeat it 5 times with different sets of target classes, as we did for the 100-classes model. For this reason the curves depicted in Fig.7 display more variability, caused by randomness in choice of classes in each of the points. Previously this variability was smoothed out by taking the average of 5 repetitions of each experiment.

The conclusions of the 100-classes scenario hold in 200-classes case, with the restriction that absolute values of accuracy of re-trained models are now a bit lower, reaching 65% in the case of all-EXT classes (comparing to 71% in 100-classes scenario).

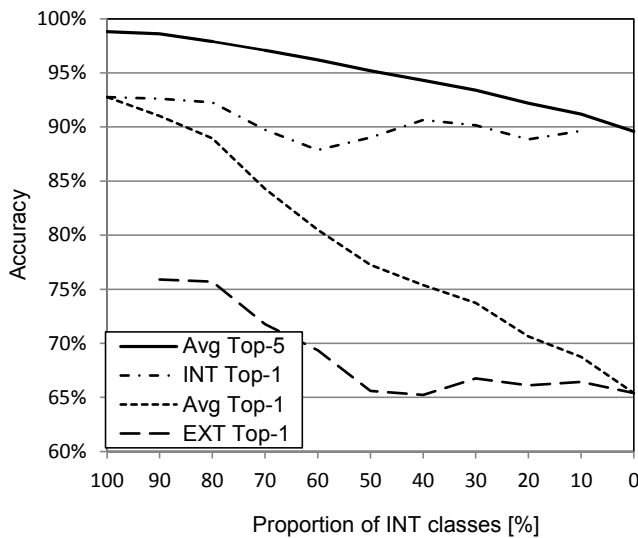


Fig. 7. Accuracy of re-trained 200-classes model with different proportion of INT and EXT classes

IV. REQUIRED NUMBER OF TRAINING EXAMPLES

An application-oriented researcher or software developer why wants to train his custom image classifier will certainly ask this important question: “How many training examples do I need to re-train the model with sufficient accuracy?”. Probably the more examples the better, but from practical perspective, large number of training examples may not be available, or may be very costly to obtain. Thus, training with limited corpus could be of interest, if the quality (accuracy) of resulting model is sufficiently good.

Aiming to answer this question we made another re-training experiment on the previously discussed 200-classes custom model, with all classes being of EXT type. However, at this time we have limited the number of training examples available in each class, starting from as few as only 3 training examples per class. For a model re-trained in such way we have measured the Top-1 and Top-5 accuracy on a test set. Then, we gradually increased the number of available training examples, up to maximum value that was about 1000 for each class (remark that for some classes Imagenet has less than 1000 examples, so in this case we have used the maximum number available).

The results, presented in Fig.8a, are a bit surprising. Clearly, the more training examples we have used, the better is the accuracy. But, apparently, with only 3 training examples per class, the Top-1 metric reaches almost 40%, and Top-5 is above 60%. This result shows that the re-trained neural network is able to extract generic visual features from images, being pre-trained on a standard image corpus. Then, having just a few training examples is sufficient to tell the model how to classify images into classes, even if the set of classes is totally different than in the original standard model.

To confirm this result, we have made similar experiment with the “standard” set of classes as defined in Imagenet1000. The achieved accuracy (see Fig.8b) is now even better, which is explained by the fact that all classes are of INT type, thus the discussed test case is not a real Transfer Learning scenario.

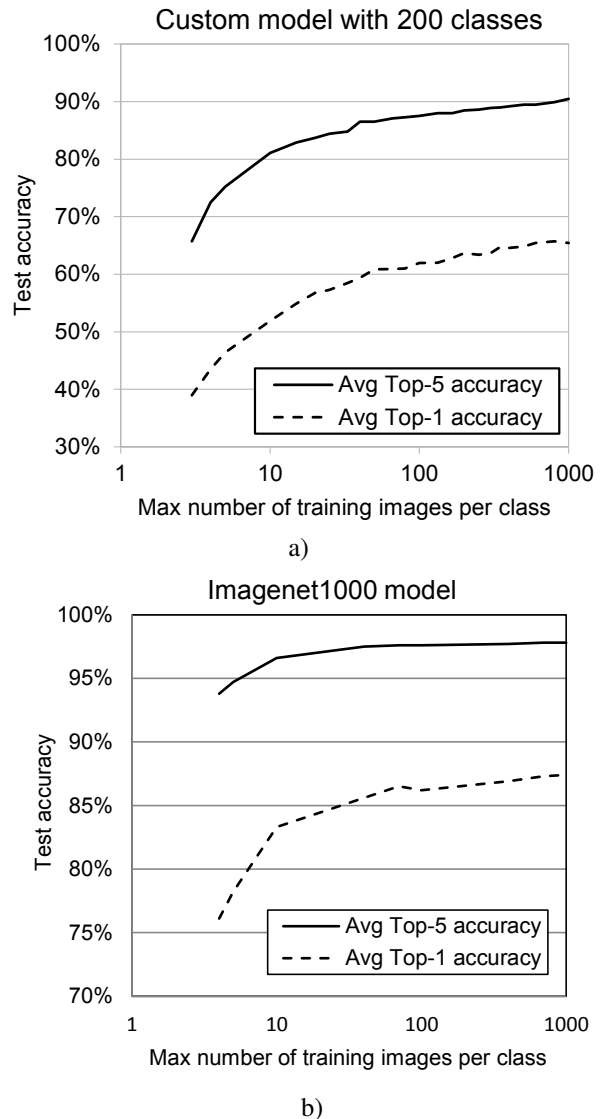


Fig. 8. Accuracy of a) custom 200-classes model, and b) Imagenet1000 model, re-trained with different number of training images per class

The reported accuracy values are averaged over all 200, or 1000 classes of a model. For this reason we don’t really know how particular classes perform. Their recognition capability may differ, depending on characteristics of particular class. For example, we may expect that telling the difference between “subway train” and “train” may be more tricky than between “train” and “cat”. This intuitively understandable differences should somehow be reflected in results of accuracy metric measured per-class.

In Fig.9 we present histogram of such per-class accuracy, in 10%-wide bins. The test was made for three different numbers of training images available per class: 3, 33 and 1000.

In the case of 1000 training images (maximum what is available) we can see that for the highest number of classes the measured Top-1 accuracy reaches between 80 and 90%. Still, there is a number of classes which seem to be problematic for image recognition model. There is 1 class with accuracy of 0%, 1 in 0-10% bin, and 4 classes in the range 10-20%.

When we limit the number of training images to 3, we can see more classes that perform poorly after re-training. Now, there are 10 classes with accuracy 0%, 26 with 0-10%, and the maximum, 31 classes, fall in the bin of 30-40%. But still, we can find 9 classes where accuracy reaches 90-100%. Clearly, there is a big discrepancy between different classes and reporting only the all-class average accuracy may be quite misleading if we want to look at one particular class.

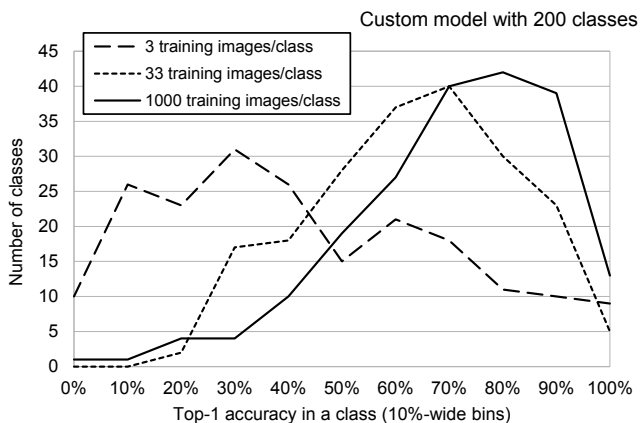


Fig. 9. Histogram of per-class accuracy in re-trained model with 200 custom classes

To look more deeply at this characteristic, we have produced a chart similar to Fig.8, but now we have divided our set of 200 target classes into several sub-sets, each with 40 classes that achieve similar per-class performance. Fig. 9 depicts the average accuracy for 3 sub-sets of classes, labeled as “easy”, “moderate” and “difficult” (referring to difficulty of classifying images of given class). Remark that the accuracy values on the figure are normalized to maximum that can be achieved for given class, because we wanted to emphasize relative differences between classes, rather than absolute values of accuracy.

We can see that the “easy” set achieves almost 90% of its maximum accuracy already with 3 training examples per class. This “easy” set contains among others such classes like:

- *Motorcycling*
- *Van, caravan*
- *Cruiser, police cruiser, patrol car*
- *Sawmill*
- *Campsite, campground, camping site*

Intuitively, these classes represent quite concrete and well-defined objects – we may easily imagine how a “motorcycle” or “van” or “sawmill” looks like. Images that belong to these classes seem to be quite “easy” for the recognizer to distinguish and so only a few training examples are enough to re-train a high quality model from the standard Imagnet1000 classifier.

The “moderate” classes achieve 50% of their maximum accuracy with only 3 training examples. The “moderate” classes are, among others:

- *Musical instrument, instrument*
- *Surveillance system*
- *Public toilet, comfort station*
- *Florist, florist shop, flower store*
- *Chairlift, chair lift*

Comparing to the first set of classes, we can intuitively see that the shape and look of “musical instrument” or “surveillance system” is not so obvious. Then, the “difficult” set achieves about 34% of its maximum accuracy with 3 training examples and it includes such classes like:

- *Plant, works, industrial plant*
- *Plaza, mall, center, shopping mall*
- *Outcrop, outcropping, rock outcrop*
- *Display window, shop window*
- *Shop, store*

A typical appearance of “shop” or “industrial plant” is not obvious at all, so difficulties in recognizing them are intuitively understandable.

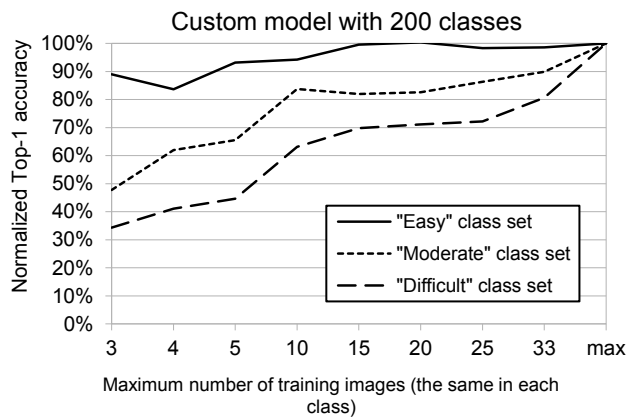


Fig. 10. Normalized accuracy vs. number of training images, for three groups of classes differing by “difficulty” of recognition

V. CUSTOM CLASSIFIER WITH MINIMUM NUMBER OF TRAINING EXAMPLES





In this experiment we focus in detail on one specific class of retrained classifier. The goal was to verify that it can indeed be trained with just as few as 3 training examples, which seemed to us unbelievable at the first time. We have added a new class, named “steering wheel”, to our custom 200-classes classifier. Such class exists in the wide Imagnet corpus, but it is not part of Imagnet1000 (so it is of EXT type).

To train the new “steering wheel” class we have decided not to use the images from Imagenet website. To make sure that we have complete control over what kind of images are used for training, we have made ourselves 3 photos of a car steering wheels, as presented in Fig.11a. These three images were used as training examples for re-training the classifier. Then, we have used 10 random images from Imagenet “steering wheel” category as a mini-test set. Fig.11b shows 4 of these test images, with final classification results. We can see that in 3 cases the class “steering wheel” indeed has the highest probability, and in 1 case it is on 3rd place in classification results.

In this simple experiment we were able to create a custom classifier to recognize “steering wheel”, and train it with just a few images. Of course, the “steering wheel” class may be considered as rather “easy” test case, since the rounded shape is visually quite characteristic. Nevertheless, the fact that in some cases just a few examples are sufficient to re-train and use a reasonably “good” model, can be of great value for potential practical deployments.



a)

	1. steering wheel (0.06)
	1. surveillance system (0.09) 2. siren (0.04) 3. steering wheel, wheel (0.04)
	1. steering wheel (0,88)
	1. steering wheel (0,31)

b)

Fig. 11. Experiment with new custom class “steering wheel”: a) training examples prepared by authors, b) testing images from Imagenet

VI. SUMMARY AND NEXT STEPS

This paper has discussed Transfer Learning method for re-training image classification models based on neural networks. Following our previous work [13], which focused on guidelines for tuning the re-training process, now we have experimentally studied performance of re-trained models, and thus the boundaries for their practical applicability.

We have shown that the re-trained model may achieve accuracy of about 70%, comparing to 90% of a fully-trained model. We think, however, that such degradation may be acceptable in some service deployments, where cost of full-scale training could be excessive. Furthermore, we have shown that the number of images required for re-training is not so big, and in the case of some “easy” classes, it could be as few as less than 10 images.

We identify several research directions as next steps:

- Continue experiments with limited number of training examples, possibly with more “difficult” classes.
- Put more attention to theoretical understanding of causes of obtained experimental results.
- Systematically compare computational cost of re-training vs. full-scale training.

We may conclude that the Transfer Learning method may be effectively used to create custom-built image classification models on top of publicly available standard ones, in a short time and with moderate cost.

REFERENCES

- [1] Ian Goodfellow, Yoshua Bengio, and Aaron Courville, “Deep Learning”, Book in preparation for MIT Press, 2016, on-line version available at:<http://www.deeplearningbook.org>
- [2] Michael A.Nielsen, “Neural Networks and Deep Learning”, Determination Press, 2015, on-line version of the book available at: <http://neuralnetworksanddeeplearning.com/index.html>
- [3] LeCun, Y., Jackel, L. D., Boser, B., Denker, J. S., Graf, H. P., Guyon, I., Henderson, D., Howard, R. E., and Hubbard, W.. Handwritten digit recognition: Applications of neural network chips and automatic learning. IEEE Communications Magazine, 27(11), 1989
- [4] A. Krizhevsky, I. Sutskever, and G. E. Hinton. ImageNet Classification with Deep Convolutional Neural Networks. In NIPS 2012, Neural Information Processing Systems, Nevada, 2012
- [5] ImageNet database of computer images: <http://image-net.org/>
- [6] Li Fei-Fei et al. ImageNet Large Scale Visual Recognition Challenge, International Journal of Computer Vision, 2015.
- [7] Ch.Szegedy et al, “Going deeper with convolutions”, <http://arxiv.org/abs/1409.4842>
- [8] Ch.Szegedy et al, Rethinking the Inception Architecture for Computer Vision, <https://arxiv.org/abs/1512.00567>
- [9] Ch.Szegedy et al, Inception-v4, Inception-ResNet and the Impact of Residual Connections on Learning, <https://arxiv.org/abs/1602.07261>
- [10] M.Abadi et al, TensorFlow: Large-scale machine learning on heterogeneous systems, 2015. Software available from tensorflow.org.
- [11] Publicly available pre-trained GoogleNet model: <https://github.com/tensorflow/models/tree/master/inception>
- [12] Yosinski J, Clune J, Bengio Y, and Lipson H. How transferable are features in deep neural networks? In Advances in Neural Information Processing Systems 27 (NIPS '14), NIPS Foundation, 2014
- [13] M.Dąbrowski, J.Gromada, T.Michalik, A practical study of neural network-based image classification model trained with transfer learning method, Position Paper of FedCSIS AIMaViG 2016, Gdańsk, September 2016, DOI: <http://dx.doi.org/10.15439/2016F211>

Topological Structures as a Tool for Formal Modelling of Rough Sets

Adam Grabowski

Institute of Informatics

Department of Mathematics and Informatics

University of Białystok,

Konstantego Ciołkowskiego 1 M, 15-245 Białystok, Poland

Email: adam@math.uwb.edu.pl

Roland Coghetto

Rue de la Brasserie, 5

B-7100 La Louvière

Belgium

Email: roland_coghetto@hotmail.com

Abstract—In the paper, we present the topological counterpart supporting rich formal apparatus describing properties of rough sets within one of the largest repositories of computerized mathematical knowledge, the Mizar Mathematical Library. The paper develops third and final (after lattice theory and the theory of general binary relations) planned path designed to be linked (via mechanisms of theory merging) with the theory of structures described by Pawlak in the early seventies of the previous century. We propose the revision of the existing topological apparatus offered by Mizar, and give the outline of the formalization of uniform spaces, important objects allowing for further representation of approximation spaces.

I. INTRODUCTION

GROWING popularity of computerized mathematical proof-assistants (Voevodsky who won the Fields medal in 2002 underlines the future of computer approach building new foundations of mathematics – univalent foundations) raises a number of new problems which should be solved in order to meet expectations of researchers. It is important that the formal approach should be flexible enough to be easily translated to writing, easily understood by people, and allow for further generalization. In recent years, traditional model of printed contribution fixed for years could be adjusted to take into account the possibilities given by contemporary media where such knowledge is stored.

We focus on the area where mathematical structures can be extensively used and their formal counterpart can be tuned accordingly. The examples were already formalized within machine-verified mathematical knowledge repository: we mean topological spaces certified with the help of the Mizar system [1].

The problem was translating these objects expressed in the natural language used by mathematicians into the formal language of Mizar. These topics are quite well represented in the Mizar Mathematical Library [15], and look promising for the mathematics as a whole – topology delivers tools for representing many other areas of mathematics (with Stone’s representation theorem at the very beginning).

II. THE MIZAR SYSTEM

The main aim of the Mizar system – the project steered by Andrzej Trybulec from early seventies of the previous

century – was to develop a formal approach to mathematics which allows for faithful encoding of the definitions and theorems written in natural language in order to be verified for correctness by computers. This formal approach should be flexible enough to be understood by ordinary people without much pain, so one of the very basic points was to be as close as possible to mathematical vernacular. On the other hand one should have in mind the strictness and the relative simplicity of the grammar of the artificial language in order to be easily scanned by the parser of the Mizar system.

The second ingredient of the system is the repository of formal texts. The Mizar Mathematical Library (MML) [27] is based on Tarski-Grothendieck set theory, which is very close to the one used by the majority of mathematicians [30]. Hence it is not very strange that general topology is one of the widely represented parts of mathematics within this repository of knowledge (see Table I for details, general topology holds fifth position w.r.t. the number of lines of code implemented, but taking into account the number of Mizar articles is just third). Among the large formalization projects of the Mizar community, two were connected with topology. The first one was the formalization of Jordan curve theorem, resulting in many articles written in tight cooperation with Japanese Mizar group (the high position held by algebraic topology – AMS MSC 2010 category started with 14 is a result of this development). The second one, the formalization of the *Compendium of Continuous Lattices* by Gierz et al. [7], although originally meant to be placed within lattice theory, eventually was driven into the direction of category theory and topology. It was quite a lucky coincidence for us as we the first author was involved also in the part dealing with the properties of Scott-continuous functions. It should be mentioned that a few well-defined topological notions, as, for example, Aleksandrov topologies, obtained a new life just with the connection with continuous domains. Another formalization project, relatively recent one, was to formalize Engelking’s *General Topology* [6], but as of now, the project seems to be not very dynamic.

Original motivation for our paper was to describe some of the issues raised in the process of formalizing important mathematical structures – topological spaces, connected with

the theory of tolerance approximation spaces [10]. We realized that in order to do this properly (at least to use as much expressive power of the Mizar language as we can), we should lift both notions into the common ground – of the descendant of topological spaces merged with approximation spaces. We have observed that developing alternative background for already well-established area of formalized knowledge can cause many troubles. This paper is a contribution to the third large area of mathematics with which rough sets are strongly linked, with another two already formalized: lattice theory [13], and general theory of binary relations [35]. Unfortunately, modal logics are not a sufficiently developed area within the Mizar Mathematical Library, and we do not expect any significant future progress in this topic.

III. TOPOLOGICAL PRELIMINARIES

A topological space is a pair (U, \mathcal{T}) consisting of a set U and family \mathcal{T} of subsets of U satisfying the following conditions:

- $\emptyset \in \mathcal{T}$ and $U \in \mathcal{T}$;
- \mathcal{T} is closed under finite intersections, i.e., for all $A, B \in \mathcal{T}$ we have $A \cap B \in \mathcal{T}$;
- \mathcal{T} is closed under arbitrary unions.

Let D be a partition of U . The collection of sets that can be written as union of some members of D together with the empty set is a topology for U – the partition topology generated by D . Obviously, every equivalence relation E generates a partition of U , namely U/E , hence it is connected with underlying topology on U . Such partition topology is usually denoted by τ_E , or just τ for fixed equivalence relation E (which is exactly the case, if we work in a given approximation space, and none other indiscernibilities are considered).

The partition topologies are characterized by the fact that every open set is also closed; every partition topology is an Alexandrov topology, in which the intersection of the members of each, not necessarily finite, collection of open sets is also open.

Let T be a tolerance relation in U and let E_T be the intersection of all equivalence relations in U that include T (extensions of T). It can be shown that E_T is again an equivalence relation, and the collection of T -definable sets is precisely the collection of E_T -definable sets. Hence, for tolerance relations T , the collection of T -definable sets is a partition topology. Essentially, the linking between an approximation space (U, E) and corresponding topological space (U, τ_E) can be established: X is definable if and only if X is open (or, respectively, closed) in the partition topology; the lower approximation of X is just the interior of X and the upper approximation of X – the closure of X . Hence X is definable if and only if its interior is equal to its closure.

The characterization of rough approximations can be also given in terms of maps between powersets of the universe U , and this was really the idea of Hammer [20]. For a binary relation R in U , the function

$$X \mapsto \{y \in U : (x, y) \in R \text{ for some } x \in X\}$$

is a mapping from 2^U into itself. Consequently then, similarly to Zhu [35], we can study the properties of approximations just by studying the properties of set-valued set-functions. In fact, the paper by Zhu [35] was fully translated into Mizar formalism and the details are to be presented at IJCRS 2017 [14].

For equivalence relation E on U a uniformity for U is defined as the collection ρ of subsets of U^2 in a following way:

$$\rho = \{R : R \subseteq U^2, E \subseteq R\}.$$

The topology for U induced by this uniformity coincides with topology τ_E . The connections between rough sets and uniform spaces [32] are as follows: Pawlak's approximation spaces are uniform spaces whose uniform topologies coincide with partition topologies; these topologies can be characterized by the fact that every open set is also closed, and hence, they are Aleksandrov topologies.

The relationship between the theory of rough sets and the theory of topological spaces is as follows: if the underlying indiscernibility relation is an equivalence relation, then the collection of definable sets is a uniformity whose topology is a partition topology (every open set is also closed and vice versa); if we deal with a tolerance relation, the collection of definable sets is a quasiuniformity whose topology is also a partition topology; if the underlying indiscernibility relation is a preorder, the collection of definable sets is a topology, but not necessarily a partition topology. In all cases however, we deal with an Alexandrov topology (arbitrary intersection of definable sets is a definable set).

IV. TOWARDS ALGEBRAIC HIERARCHY

All algebraic structures in Mizar are defined in similar manner: first we have to give a structure, where names of fields (called selectors) with their specification (the type and the arity) are given. In our concrete case there were

```

definition
  struct (1-sorted) addMagma
    (# carrier -> set,
      addF -> BinOp of the carrier #);
end;
and
definition
  struct (ZeroStr, addMagma) addLoopStr
    (# carrier -> set,
      addF -> BinOp of the carrier,
      ZeroF -> Element of the carrier #);
end;

```

Structures in Mizar can be used to model mathematical notions like groups, topological spaces, categories, etc. which are usually represented as tuples. A structure definition contains, therefore, a list of *selectors* to denote its fields, characterized by their name and type, e.g.:

```

definition
  struct multMagma
    (# carrier -> set,

```


TABLE I
TOP 10 DEVELOPED THEORIES IN MML BY AMS MSC 2010

No.	MSC	Topic	Number of articles	Lines of code
1.	03	Mathematical logic and foundations	146	311,083
2.	14	Algebraic geometry	84	251,809
3.	06	Order, lattices, ordered algebraic structures	110	234,413
4.	26	Real functions	91	225,634
5.	54	General topology	99	196,486
6.	68	Computer science	83	193,782
7.	11	Number theory	72	154,307
8.	15	Linear and multilinear algebra; matrix theory	61	149,941
9.	46	Functional analysis	69	132,741
10.	57	Manifolds and cell complexes	42	122,738

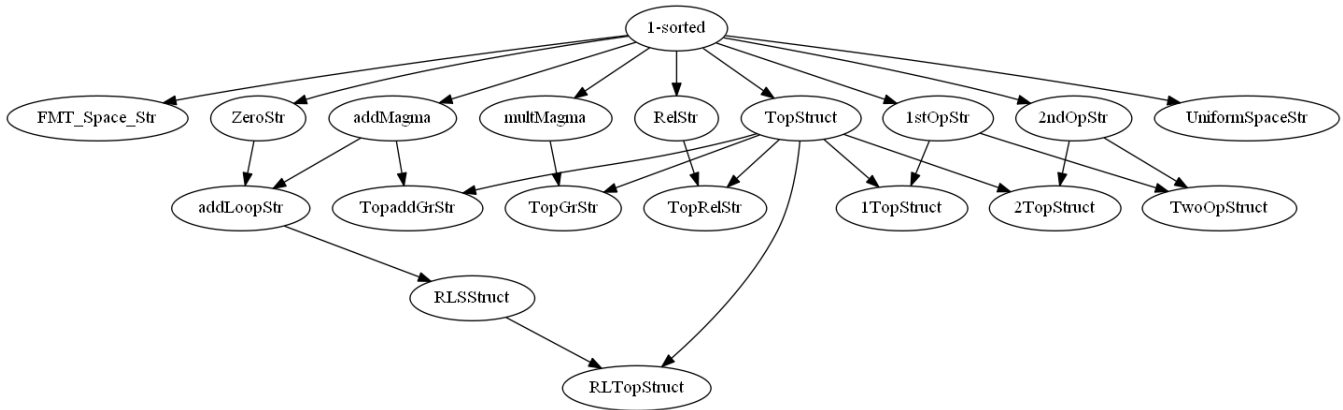


Fig. 1. The net of topological structures in MML

```
multF -> BinOp of the carrier #);
end;
```

where `multMagma` is the name of a structure with two selectors: an arbitrary set called its `carrier` and a binary operation on it, called `multF`. This structure can be used to define a group, but also upper and lower semilattices, so in fact any notion that is based on a set and a binary operation on it. It should be noted that the above structure does not define a group yet (nor any other more concrete object), because there is no information on the properties of `multF`. The structure is just a basis for developing a theory. In practice, after introducing a required structure, a series of attributes is also defined to describe the properties of certain fields.

As mentioned before, the above `multMagma` structure can be used to define notions which are not only groups. Still, the operation in such structures inherit the name `multF`, because the current Mizar implementation does not provide a mechanism to introduce synonyms for selectors (or whole structures). Therefore, in cases when a different name is frequently used in standard mathematical practice, it may be better to introduce a different structure. For example, lattice operations are commonly called `meet` and `join`, so a lower semilattice may be better encoded as:

```
definition
  struct /\-SemiLattStr
    (# carrier -> set,
```

```
L_meet -> BinOp of the carrier #);
end;
```

Mizar supports multiple inheritance of structures that makes a whole hierarchy of interrelated structures available in the Mizar library, with the `1-sorted` structure being the common ancestor of almost all other structures. For example, formalizing topological groups in Mizar can be done by independently defining and developing group theory and the theory of topological spaces, and then merging these two theories together based on a new structure, e.g.:

```
definition
  struct (1-sorted) TopStruct
    (# carrier -> set,
      topology -> Subset-Family of the carrier
    #);
end;

definition
  struct (multMagma, TopStruct) TopGrStr
    (# carrier -> set,
      multF -> BinOp of the carrier,
      topology -> Subset-Family
        of the carrier #);
end;
```

The advantage of this approach is that all notions and facts concerning groups and topological spaces are naturally applicable to topological groups. Let us note that when introducing a new structure, the inherited selectors can be listed in any

order, as far as relations between them are preserved. The list of names of ancestor structures is put in brackets before the name of the structure being defined. Figure 1 shows only the part of the net of all over 150 structures defined in MML which are used for formalizing topology: we can find there topological groups, topological relational structures, or real linear spaces equipped with a topology, just to mention a few important ones. Structures `RelStr` and `TopStruct` are in the middle as the most important ones, and crucial in the formalization of CCL. The right hand side of the diagram was recently fully developed by the authors; it is useful both for alternative formal approach to topological spaces which will be shown in Section VII and the theory of uniform spaces given by the second author.

Concrete mathematical objects, e.g. the additive group of integers are introduced with so called *aggregates* – special term constructors defined automatically by the definition of a structure, e.g.: `multMagma(#INT, addint#)`, where `INT` is the set of integers, and `addint` represents the addition function. It is necessary that all terms used in the aggregate have the respective types declared in the structure’s definition. In our example `INT` is obviously a set, and `addint` must be of type `BinOp of INT`.

Every structure defines implicitly a special attribute, `strict`. The corresponding adjective’s meaning is that an object of a structure type contains nothing more, but the fields defined for that structure. For example, a term with structural type based on `TopGrStr` may be `strict TopGrStr`, but it is neither `strict multMagma`, nor `strict TopStruct`. Clearly, every term constructed using a structure’s aggregate is `strict`.

Finally, the Mizar language has means to restrict a given term with a complex structure type to its well-defined subtype. This special term constructor, the *forgetful functor* also utilizes the structure’s name, e.g. the `multMagma of G`, where `G` has a potentially wider type which inherits the `multMagma` structure. Again, such terms are `strict`, with respect to the given structure type. The (part of) hierarchy of algebraic structures deliver only a signature for corresponding algebras; the real semantics is given by axioms. In Mizar formalism, axioms are defined as adjectives (called also attributes). The details of the algebraic hierarchy in the Mizar Mathematical Library were presented at FedCSIS conference last year [17].

V. TOPOLOGY FORMALIZED

In this section we will describe the existing current definition of topological spaces within MML. Following Engelking [6], we can choose open sets as the basic notion and so it was decided to be the base in the MML: we have a structure of a topological space together with the only adjective of which name suggests its technical character. We can originally choose between point-free topology and that with points; in MML we deal with the earlier approach. Obviously, the backbone corresponding structure is `TopStruct` given in Section IV. Similarly, as in the algebraic case, structures can be understood as partial functions on the selectors (in the abovementioned example, the carrier which is a set on which a topology can

be defined, and the topology, i.e. the family of open sets). But the real properties of the topology (both \emptyset and the whole universe should be open; the family should be closed for finite intersections and arbitrary unions) is given by the Mizar attribute which is in fact an adjective (`TopSpace-like`).

```
definition let IT be TopStruct;
  attr IT is TopSpace-like means
:: PRE_TOPC:def 1
  the carrier of IT in the topology of IT &
  (for a being Subset-Family of IT st
   a c= the topology of IT holds
   union a in the topology of IT) &
  for a,b being Subset of IT st
   a in the topology of IT &
   b in the topology of IT holds
   a /\ b in the topology of IT;
end;
```

Making appropriate hierarchy for well-established notions is really crucial for the repository of formal texts; if we are interested only in pure predicates and computer-generated proofs, readability is something which does not really matters (and this is the case of the part of Isabelle’s Archive of Formal Proofs [3] devoted to software verification), however from a viewpoint of reusability of adjectives, when large databases are involved, this is a question of efficiency. As a simple nontrivial example, we can mention the net of cross-linked properties of rough approximation operators under various conditions as reflexivity, symmetry, transitivity – as canonical examples, but also with seriality, positive and negative alliance as less straightforward ones.

We can see that essentially the whole series of Mizar articles dealing with topology uses more or less the type defined as the structure with the single adjective as described in this section – the Mizar mode `TopSpace` is not very convenient starting point for further generalizations. One can notice that we do not need in the abovementioned definition the assumption that the empty set is an element of the topology: the union of \emptyset is just \emptyset , and the thesis is trivial as any topology is closed under arbitrary unions. Bourbakists define topological spaces just by means of finite intersections and arbitrary unions, but one the other hand the set $\bigcap \emptyset$ is not well-defined in Zermelo-Fraenkel set theory.

We can see a topological operator either from the view of Mizar functors, as it can be recognized now as a base; as they are typed, we can read that the closure of an arbitrary subset of given topological space T is again the subset of T . But alternatively, we can use another way around: first we can define a function which returns the closure for arbitrary argument. Of course, one should define for such a map the domain and the range properly; in our specific case this could be a (total) function defined on the boolean of the carrier of T . Among various approaches to topological spaces the two are especially important: the first one deals with the family of subsets of a given universe possessing certain properties; the other deals with closure operators in sense of Kuratowski.

```
definition
  let T be TopStruct,
```

```

P be Subset of T;
attr P is open means
:: PRE_TOPC:def 2
P in the topology of T;
end;

```

Closed sets are precisely those, of which complements are open; similarly the closure of given subset A can be defined just as the minimal closed set containing A .

```

definition
let GX be TopStruct, A be Subset of GX;
func Cl A -> Subset of GX means
:: PRE_TOPC:def 7
for p being set st p in the carrier of GX
holds
p in it iff for G being Subset of GX st
G is open holds p in G
implies A meets G;
end;

```

Of course, the above is definitely not the only possible definition – we can define the closure as the intersection of all closed supersets of A , but the obvious and important connection between the closures and closed sets is that closed subsets are fixed points with respect to the closure operators.

```

theorem :: PRE_TOPC:22
for A being Subset of T holds
(A is closed implies Cl A = A) &
(T is TopSpace-like & Cl A = A implies
A is closed);

```

As a consequence, the above theorem can be considered as an equivalent definition of a closed set as the fixed point under closure operator; this will be explained from another viewpoint (and reused) later.

We can mention here the outline of the formalization of the common generalization of topological groups and metric spaces. Uniform spaces, which are credited to Weil [33] and more systematic formal approach – to the group of Bourbakists (which is quite nice coincidence as the Mizar project implements main postulates of formalization of mathematics which were fundamental to Bourbaki group), appeared to be a useful framework explaining the concept of rough sets in terms of both equivalence and tolerance relations. Formally, uniform spaces are based on Mizar structures

```

definition
struct (1-sorted)
UniformSpaceStr
(# carrier -> set,
entourages -> Subset-Family of
[:the carrier,the carrier:] #);
end;

```

where French *entourages* means surroundings. The real topological flavour of these pretty general constructions is given by defining an open subset O of X if and only if for every $x \in O$ there exists an entourage V such that $V[x]$ is a subset of O . For more details of fundamental systems of entourages treated formally, we refer to [4] and [5] containing thorough encoding of the theory – almost 7 thousand lines of code, i.e. about 90 pages of formal definitons, theorems, and proofs.

The essential notion is the uniformity induced by the general binary relation

```

definition
let X be set,
R be Relation of X;
func uniformity_induced_by(R) ->
upper cap-closed strict UniformSpaceStr
equals
:: UNIFORM3:def 21
UniformSpaceStr (# X,rho(R) #);
end;

```

where ρ is just ρ as described in Section III. Adding underlying properties to a binary relation, it turns out that we obtain axioms defining basic classes of (semi-)uniform spaces. The full connection between theory of uniform spaces and rough sets is expressed in two important corollaries:

```

definition
let X be set,
R be Tolerance of X;
redefine func uniformity_induced_by(R)
-> strict Semi-UniformSpace;
end;

```

```

theorem :: UNIFORM3:51
for X being set,
R being Equivalence_Relation of X
holds
uniformity_induced_by(R) is UniformSpace;

```

Even if usually uniform spaces are meant to be topological spaces with additional structure, this extension is absent in the above definition, as this time we presented purely topological properties in terms of Mizar adjectives (instead of fixed topology we use appropriate notions in terms of entourages, which is not very strange, as we can use the notion of a neighbourhood).

VI. THE ISSUE OF EQUIVALENT CHARACTERIZATIONS

In mathematics we often experience the situation when we have equivalent sets of axioms for the same mathematical object. The motivation of using them both in the same time can be manifold: either the approaches were developed in a sense independently, without knowing each other, and after that they were proved to be equivalent definitions of the same notion, or just the newly proposed set is preferred because of its simplicity or usefulness. Such considerations are especially often in lattice theory, where we deal with the fixed set of operations (as the supremum, the infimum and the complementation). The situation gets slightly more complicated if the collections of operations are distinct. Of course, the canonical example here is delivered again in the world of lattices, where we have, among the ordinary binary operations \sqcup and \sqcap (or, to be more precise, instead of them at first) the ordering relation \leq . In this case, the original idea to show the correspondence was to define two Mizar functors transforming posets into lattices [12], [18], and vice versa.

When we consider things informally, it is enough to have such construction; but then, we cannot be in these two universes in the same time and we have to choose only a single

framework to work with (and redefine construction really supports such approach). Some time ago, as a part of the formalization of Jordan curve theory, we did similar work: essentially we have shown that the notion of an open set defined for subset of the set of real numbers coincides with that of an open set in the natural topology of the real line. Of course, having basic properties proven in both settings is important, but soon we should face the problem of how much theory to be developed in parallel.

As an interesting direction of research in the area of topology [8] we can point out the beginnings of the so-called theory of finite topological spaces as defined by Imura and Eguchi in [22]. Based on relational structures, the authors define new operator which is just the set of all elements of the universe which are in the internal relation with the given point.

```
definition
  let FT be RelStr;
  let x be Element of FT;
  func U_FT x -> Subset of FT equals
:: FIN_TOPO: def 1
  Class (the InternalRel of FT, x);
end;
```

The Mizar functor `Class` meant originally the class of abstraction w.r.t. the given equivalence relation. In the process of generalizing notions all underlying attributes were removed from the assumptions of this definition, but the name remains the same. One of the basic properties of neighbourhoods states that any point should be a member of its neighbourhood. Although the above definition does not need any additional assumptions, now we have to add a variant of reflexivity of the relational structure, with the new synonymical name, `filled`. Of course, having just a new name for the old notion does not bring too much additional information; but now we can express the reflexivity in terms of neighbourhoods.

```
definition
  let IT be non empty RelStr;
  redefine attr IT is filled means
:: FIN_TOPO: def 4
  for x being Element of IT holds x in U_FT x;
end;
```

The series started with [22] is not really exhaustive; but the connections with other areas of mathematics are obvious.

VII. THE NEW APPROACH

The first step in our proposed approach was to have the new naming scheme. We decided to use again a postfix `-like` to suggest that if a family of subsets satisfies the conjunction of properties, it can be treated as the family of open sets (i.e. it is a topology).

```
definition
  let X be set;
  let F be Subset-Family of X;
  attr F is topology-like means
  {} in F & X in F &
  F is union-closed cap-closed;
end;
```

Later, such adjectives were meant to be replaced by more selfexplaining names. But in fact, the first conjunct is just the negation of already present in MML `with_non-empty_elements`, and the second one can be named as `with_universe` or something similar. Observe that there are two main differences between the definition from Section V (`TopSpace-like`) and the current one. The first one is that the latter is on the concrete level, i.e. it does not use the notion of the structure. Of course, it is easy to lift such definition to the abstract (i.e. structural) level: one can define appropriate field to have such properties. The second difference is that the old one is the conjunction of three instead of four adjectives, as one of them can be deduced from the combination of remaining ones and in this sense the approach proposed here is similar to the one developed in the case of σ -fields of subsets. In such a manner, we deal with Čech preclosure and Kuratowski closure operators, respectively.

```
definition
  let X be set,
  O be Function of bool X, bool X;
  attr O is preclosure means
  O is extensive \/-preserving
  empty-preserving;
  attr O is closure means
  O is extensive idempotent
  \/-preserving empty-preserving;
end;
```

The crucial issue here is about the structure on which we can establish the connection between closed sets and fixed points w.r.t. maps. We decided not to use concrete relational structures, but we introduced new structures, `1TopStruct` which are ancestors of topological structures enriched by maps on X , i.e. functions from the set 2^X into itself.

```
theorem :: ROUGHS_4:2
  for T being with_properly_defined_topology
  1TopStruct,
  A being Subset of T holds
  A is op-closed iff A is closed;
```

Under such defined attributes, showing that if the operator satisfies the properties of preclosure, it generates an abstract topological space.

```
registration
  cluster with_preclosure -> TopSpace-like for
  with_properly_defined_topology 1TopStruct;
end;
```

The question of defining the family of open sets (i.e. the most usual definition of topology) might arise; the answer is immediate – as the family of fixed points under the closure operator. So the topology is collected from these objects which are subsets of the considered universe which are f -closed, where f stands for the map under consideration (an abstract closure operator).

```
definition
  let X be set,
  f be Function of bool X, bool X;
  func GenTop f -> Subset-Family of X means
```

```

:: ROUGHS_4:def 25
  for x being object holds
    x in it iff ex S being Subset of X st
      S = x & S is f-closed;
end;

```

In fact, this is another formulation of the property expressed by the attribute `with_properly_defined_topology`.

```

theorem :: ROUGHS_4:5
  for X being set,
  f being Function of bool X, bool X st
  f is preinterior holds
  GenTop f is topology-like;

registration
  let C be set, I be (Relation of C),
  f be topology-like Subset-Family of C;
  cluster TopRelStr (#C,I,f#) -> TopSpace-like;
end;

```

Finally, composing the above theorem and functor registration, we deduce that if the map which is the field in the merged structure had the properties of preclosure, generated space has all the properties of topological spaces.

VIII. MERGING TOPOLOGIES AND ROUGH SETS

The notion of a rough set was defined by Pawlak [28] to reflect the situation of an incomplete knowledge about the universe of objects. We formalized the notion in Mizar [11] and pretty recently observed that this is almost identical to the approach described in Section VI. Any element of the universe can be viewed through a binary relation which can unify potentially distinct objects if the available information about their properties is the same. Such relation, called indiscernibility relation, can possess basic mathematical properties of relations: if we assume R to be reflexive, symmetric, and transitive (so it is an equivalence relation), we have the original approach of Pawlak.

```

definition let T be non empty TopRelStr;
  attr T is naturally_generated means
:: ROUGHS_4:def 28
  the topology of T = GenTop LAp T;
end;

theorem :: ROUGHS_4:10
  for T being naturally_generated
  non empty with_equivalence TopRelStr,
  A being Subset of T holds
  A is closed iff UAp A = A;

```

As both notions coincide (the upper approximation operator in rough sets and closure operator in underlying topological spaces and similarly in the dual case), reusing these areas of mathematics we have obtained concrete results: the characterization of rough sets in terms of Isomichi classification of domains, and the view for rough sets from the viewpoint of Kuratowski closure-complement problem (known also as fourteen sets of Kuratowski) [9].

As always, we can be skeptical about defining the mathematical object as one of the fields in the structure: it could be well illustrated based on the notion of the complementation

operator in the lattice structure. On the one hand, it is really natural to have it as a separate field, as it was in case of ortholattices. When it is just a part of the language's signature, it reflects the ordinary mathematical definition [16].

```

registration
  let T be naturally_generated
  non empty with_equivalence TopRelStr,
  A be Subset of T;
  cluster UAp A -> closed;
end;

registration
  let T be with_equivalence
  naturally_generated non empty TopRelStr;
  let A be Subset of T;
  identify Cl A with UAp A;
end;

```

The latter registration would allow for mixed use of the lower approximation instead of interior operator and vice versa. The only drawback of this approach is that to obtain pure context of uniform space (i.e. strict topological space or strict tolerance approximation space), we have to use Mizar forgetful functor `the`.

The above unification of the world of topological spaces and of rough sets allowed us to fully benefit from the results placed in the area of general topology, previously obtained: we can easily observe the connection of approximation spaces with the classification of domains proposed by Isomichi or the problems of Kuratowski sets, giving the combination of closure, interior, and complementation operators [11], without explicit reference to those theories.

IX. CONCLUSION AND FUTURE WORK

In the paper we tried to show how theoretically straightforward examples can lead to difficult problems during their translation from informal presentation in natural human language into formalism of the Mizar language, a variant of mathematical vernacular. Based on the example of topological spaces we could observe that even if the approach is given in a not satisfactory way, it can be corrected in a process of the so-called revision [19]. The part of the work could be less painful – the splitting of the original definition as we proposed and automatic replacement of the references into new ones. The level of generality is obviously higher in our approach, so we hope to open some new paths in the formalization of general topology, especially in more abstract form.

The second part, which could be done gradually and with the possible use of automatic tools, is that this proposed new version should be consumed in the MML – the theorems and definitions which can be formalized in the more general way, should be formulated so. This would also enable reusing purely topological constructions in another areas of mathematics – for example, fourteen Kuratowski sets can be expressed in the language of group theory and abstract maps with accompanying properties. This also opened the way for explaining rough sets in topological terms and will not be restricted for the Mizar library only, as the translation from the Mizar formalism

into other formal languages are available [21]. Additionally we hope to unify the existing approach with newly developed theory of uniform spaces.

In the informal form of a mathematical publication written by people in natural language, such process could (and eventually led in real life, as it was in the world of rough sets) to the sequence of papers generalizing the approach gradually. Hence it is also a kind of a problem for repository storing the knowledge. In our case, the Mizar Mathematical Library allows for some automatic enhancements. We removed repetition, compressed the files, and cleared the path to improve the overall algebraic framework available in the Mizar Mathematical Library. Although natural language is rather flexible, we believe that formal counterpart benefits from the relative coherence of the existing approaches.

REFERENCES

- [1] Bancerek, G., Byliński, C., Grabowski, A., Kornilowicz, A., Matuszewski, R., Naumowicz, A., Pał, K., and Urban, J. (2015). Mizar: State-of-the-art and beyond. In Kerber, M., Carette, J., Kaliszky, C., Rabe, F., and Sorge, V., editors, *Intelligent Computer Mathematics – International Conference, CICM 2015, Washington, DC, USA, July 13–17, 2015, Proceedings*, volume 9150 of *Lecture Notes in Computer Science*. Springer, pages 261–279. doi:10.1007/978-3-319-20615-8_17
- [2] Bancerek G, Rudnicki P. (2002). A Compendium of Continuous Lattices in Mizar (formalizing recent mathematics). *Journal of Automated Reasoning*, 29(3/4):189–224. doi:DOI: 10.1023/A:1021966832558
- [3] Blanchette, J., Haslbeck, M., Matichuk, D., and Nipkow, T. (2015). Mining the Archive of Formal Proofs, in Kerber, M., editor. *Conference on Intelligent Computer Mathematics (CICM 2015)*, Lecture Notes in Computer Science, 9150, pages 3–17, Springer. doi:10.1007/978-3-319-20615-8_1
- [4] Coghetto, R. (2016). Quasi-uniform space. *Formalized Mathematics*, 24(3):215–226. doi:10.1515/forma-2016-0017
- [5] Coghetto, R. (2016). Uniform space. *Formalized Mathematics*, 24(3):205–214. doi:10.1515/forma-2016-0018
- [6] Engelking, R. (1977). *General Topology*, volume 60 of *Monografie Matematyczne*. PWN – Polish Scientific Publishers, Warsaw.
- [7] Gierz, G., Hofmann, K., Keimel, K., Lawson, J., Mislove, M., and Scott, D. (1980). *A Compendium of Continuous Lattices*. Springer-Verlag, Berlin, Heidelberg, New York.
- [8] Grabowski, A. (2004). Solving two problems in general topology via types. In Filliâtre, J., Paulin-Mohring, C., and Werner, B., editors, *Types for Proofs and Programs, International Workshop, TYPES 2004, Jouy-en-Josas, France, December 15–18, 2004, Revised Selected Papers*, volume 3839 of *Lecture Notes in Computer Science*, pages 138–153. Springer. doi:10.1007/11617990_9
- [9] Grabowski, A. (2005). On the computer-assisted reasoning about rough sets. In Dunin-Kępicz, B., Jankowski, A., Skowron, A., and Szczuka, M., editors, *International Workshop on Monitoring, Security, and Rescue Techniques in Multiagent Systems Location*, volume 28 of *Advances in Soft Computing*, pages 215–226, Berlin, Heidelberg. Springer-Verlag. doi: 10.1007/3-540-32370-8_15
- [10] Grabowski, A. (2013). Automated discovery of properties of rough sets. *Fundamenta Informaticae*, 128(1-2):65–79. doi:10.3233/FI-2013-933
- [11] Grabowski, A. (2014). Efficient rough set theory merging. *Fundamenta Informaticae*, 135(4):371–385. doi:10.3233/FI-2014-1129
- [12] Grabowski, A. (2015). Mechanizing complemented lattices within Mizar type system. *Journal of Automated Reasoning*, 55(3):211–221. doi:10.1007/s10817-015-9333-5
- [13] Grabowski, A. (2016). Lattice theory for rough sets – a case study with Mizar. *Fundamenta Informaticae*, 147(2–3):223–240. doi:10.3233/FI-2016-1406
- [14] Grabowski, A. (2017). Computer certification of generalized rough sets based on relations. Accepted to International Joint Conference on Rough Sets, IJCRS 2017. doi:10.1007/978-3-319-60837-2_7
- [15] Grabowski, A., Kornilowicz, A., and Naumowicz, A. (2015). Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198. doi:10.1007/s10817-015-9345-1
- [16] Grabowski, A., Kornilowicz, A., and Schwarzweller, C. (2015). Equality in computer proof-assistants. In Ganzha, M., Maciaszek, L. A., and Paprzycki, M., editors, *Proceedings of the 2015 Federated Conference on Computer Science and Information Systems*, volume 5 of *Annals of Computer Science and Information Systems*, pages 45–54. IEEE. doi:10.15439/2015F229
- [17] Grabowski, A., Kornilowicz, A., Schwarzweller, C. (2016). On algebraic hierarchies in mathematical repository of Mizar. In: M. Ganzha, L.A. Maciaszek, M. Paprzycki, editors, *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems*, volume 8 of *Annals of Computer Science and Information Systems*, pages 363–371. IEEE. doi:10.15439/2016F520
- [18] Grabowski, A. and Moschner, M. (2004). Managing heterogeneous theories within a mathematical knowledge repository. In Asperti, A., Bancerek, G., and Trybulec, A., editors, *Mathematical Knowledge Management, Third International Conference, MKM 2004, Bialowieza, Poland, September 19–21, 2004, Proceedings*, volume 3119 of *Lecture Notes in Computer Science*, pages 116–129. Springer. doi:10.1007/978-3-540-27818-4_9
- [19] Grabowski, A. and Schwarzweller, C. (2007). Revisions as an essential tool to maintain mathematical repositories. In *Proceedings of the 14th Symposium on Towards Mechanized Mathematical Assistants: 6th International Conference*, Calculemus '07 / MKM '07, pages 235–249, Berlin, Heidelberg. Springer-Verlag. doi:10.1007/978-3-540-73086-6_20
- [20] Hammer, P.C. (1963). Extended topology: the continuity concept. *Mathematics Magazine*, 36(2):101–105.
- [21] Iancu, M., Kohlhase, M., Rabe, F., and Urban, J. (2013). The Mizar Mathematical Library in OMDoc: Translation and applications. *Journal of Automated Reasoning*, 50(2):191–202. doi:10.1007/s10817-012-9271-4
- [22] Imura, H. and Eguchi, M. (1992). Finite topological spaces. *Formalized Mathematics*, 3(2):189–193.
- [23] Järvinen, J. (2007). Lattice theory for rough sets, *Transactions on Rough Sets VI*, Lecture Notes in Computer Science (LNAI) 4374:400–498. doi:10.1007/978-3-540-71200-8_22
- [24] Kornilowicz, A. (2015). Definitional expansions in Mizar. *Journal of Automated Reasoning*, 55(3):257–268. doi:10.1007/s10817-015-9331-7
- [25] Kornilowicz, A. (2015). Flexary connectives in Mizar. *Computer Languages, Systems & Structures*, 44:238–250. doi:10.1016/j.cl.2015.07.002
- [26] Naumowicz, A. (2015). Automating Boolean set operations in Mizar proof checking with the aid of an external SAT solver. *Journal of Automated Reasoning*, 55(3):285–294. doi:10.1007/s10817-015-9332-6
- [27] Naumowicz, A. (2015). Tools for MML environment analysis. In Kerber, M., Carette, J., Kaliszky, C., Rabe, F., and Sorge, V., editors (2015). *Intelligent Computer Mathematics – International Conference, CICM 2015, Washington, DC, USA, July 13–17, 2015, Proceedings*, volume 9150 of *Lecture Notes in Computer Science*. Springer, pages 348–352. doi:10.1007/978-3-319-20615-8_26
- [28] Pawlak, Z. (1982). Rough sets. *International Journal of Parallel Programming*, 11:341–356.
- [29] Pał, K. (2015). Improving legibility of formal proofs based on the close reference principle is NP-hard. *Journal of Automated Reasoning*, 55(3):295–306. doi:10.1007/s10817-015-9337-1
- [30] Trybulec, A., Kornilowicz, A., Naumowicz, A., and Kuperberg, K. (2013). Formal mathematics for mathematicians. *Journal of Automated Reasoning*, 50(2):119–121. doi:10.1007/s10817-012-9268-z
- [31] Urban, J., Rudnicki, P., and Sutcliffe, G. (2013). ATP and presentation service for Mizar formalizations. *Journal of Automated Reasoning*, 50(2):229–241. doi:10.1007/s10817-012-9269-y
- [32] Vlach, M. (2008). Topologies of approximation spaces of rough set theory, In *Interval/Probabilistic Uncertainty and Non-Classical Logics*, pp. 176–186, *Advances in Soft Computing*, 46, Springer. doi: 10.1007/978-3-540-77664-2_14
- [33] Weil, A. (1937). Sur les espaces a structure uniforme et sur la topologie generale. *Act. Sci. Ind.*, 551, Paris.
- [34] Yao, Y., Yao, B. (2012). Covering based rough set approximations, *Information Sciences*, 200:91–107. doi:10.1016/j.ins.2012.02.065
- [35] Zhu, W. (2007). Generalized rough sets based on relations, *Information Sciences*, 177(22):4997–5011. doi:10.1016/j.ins.2007.05.037
- [36] Zhu, W. (2007). Topological approaches to covering rough sets, *Information Sciences*, 177(6):1499–1508. doi:10.1016/j.ins.2006.06.009

Direct Potentiality Assimilation for Improving Multi-Layered Neural Networks

Ryotaro Kamimura, IT Education Center, Tokai University
4-1-1 Kitakaname, Hiratsuka, Kanagawa 259-1292, Japan
ryo@keyaki.cc.u-tokai.ac.jp

Abstract—The present paper aims to propose a new potential learning method to overcome the problem of collective interpretation for interpreting multi-layered neural networks. The potential learning has been introduced to detect important components of neural networks and to train them, taking into account the importance of components. Recently, it has been applied to multi-layered neural networks and then the interpretation of input neurons or variables can be possible by collectively treating intermediate layers. However, the collective interpretation for multi-layered neural networks tends to be instable, because the potentialities computed in the pre-training become different from those in the main training. To overcome this problem, we introduce the potential learning with direct potential assimilation. The direct potential assimilation means that the potentiality assimilation is not applied in the phase of pre-training but it is applied directly to training multi-layered neural networks. The new method was applied to the student evaluation data set. Then, it was observed that the selectivity of connection weights could be increased. Then, the input-output potentiality was quite similar to the regression coefficients of logistic regression analysis. Finally, the new method could extract more explicitly input-output relations than the regression coefficients by the logistic regression analysis, while improving generalization performance.

I. INTRODUCTION

A. Problem of Collective Interpretation

NEURAL networks have been well known for their inability to interpret final results [1], [2], [3], [4], [5]. Thus, compared with conventional logistic analysis, the neural networks have not been necessarily used in many practical problems. This hard interpretation has become much more serious for multi-layered neural networks. Some results on interpretation were reported [6], [7], but the majority were heavily based on the characteristics of input patterns. For example, when the inputs are images, they can be easily interpreted intuitively by the conventional visualization methods. Particularly, in multi-layered neural networks, it has been difficult to interpret the intermediate layers.

For interpretation, we have so far introduced potential learning [8], [9], [10] where the importance of neural components is determined before learning, and they are assimilated in connection weights. Potential learning has been developed to simplify the computational procedures of information-theoretic methods [11], [12], [13], [14]. The potential learning has been recently extended to multi-layered neural networks. As above mentioned, for the multi-layered neural networks, the problem becomes more serious, particularly, for interpretation. Even in the case of single-layered neural networks, the interpretation is

not so easy that we need very special types of procedures for interpretation. In multi-layered neural networks, the complicated behaviors of many intermediate layers cannot be easily interpreted. To simplify the interpretation of multi-layered neural network, we focus on relations between inputs and outputs by treating collectively all intermediate layers. This is because in many applications, we must examine how input variables (neurons) are related to the corresponding outputs [15], [16], [17]. Thus, we try to estimate how input neurons have influences on outputs by considering all intermediate layers.

However, the problem of this collective interpretation is that the interpretation has been unstable because of unstable potentialities. The instability of final results is due to the fact that the connection weights, obtained in the pre-training, can be changed in the fine-tuning or main-training. Thus, even if the potentiality of neural components is rigorously computed, it can be of no use in main-training. For this problem, we have introduced direct potentiality assimilation where the potential learning focuses not on pre-training but on main-training. In our new method, the roles of pre-training are reduced as much as possible.

B. Direct Potentiality Assimilation

The instability problem, inherent to the potentiality learning or assimilation, can be solved by transferring the potentiality assimilation from the pre-training to the main-training. Since the method directly apply the potentiality to the main-training, it is called “direct potentiality assimilation”. In the ordinary deep learning, the un-supervised or semi-supervised learning such as auto-encoders is used for the pre-training. In the pre-training using the auto-encoders, the potentiality must be assimilated by repeating the assimilation processes, because the effect of potentiality tends to disappear. Then, we have the fine-tuning or main-training with connection weights by the pre-training. The problem is that the information on input patterns tends to disappear in the time of pre-training, because of the repeated assimilation. This means that the original information on inputs tends to disappear in the pre-training, and thus connection weights, transferred to the main-training, happen to have little information on input patterns, leading to the instability of learning and interpretation. To overcome this problem, we transfer the process of assimilation to the main training. Then, in the pre-training, no regularization can be implemented and we try to obtain the overall or

rough information on input patterns. In the main-training, the important connection weights in terms of potentiality is extracted and assimilated fully.

C. Paper Organization

In Section 2, we first explain conceptually direct and indirect potential learning and then how to compute the potentiality and how to assimilate the potentiality into connection weights. For the collective interpretation, we present how to deal collectively with intermediate layers by considering only positive weights. In Section 3, the student evaluation data set was used where we try to show that the selectivity could be improved, with better generalization performance. In addition, the collective weights were found to be very similar to those by the logistic regression analysis. Finally, the method could successfully extract the clearer roles of input neurons or variables.

II. THEORY AND COMPUTATIONAL METHODS

A. Direct and Indirect Potential Learning

In the previous models, we applied the potential learning to multi-layered neural networks indirectly. This means that the potential learning was applied to the pre-training phase. The problem of this indirect method is that the information on input patterns tends to disappear in the phase of pre-training. The multi-layered neural networks themselves tend to lose the original information when going through many different layers, as pointed out and well-known in the field of information theory [18], [19], [20]. In addition, the weight decay and sparse constraints [21], [22], [23], [24], usually used in the pre-training, naturally tend to lose the original information, because those methods try to simplify the complexity of networks by decreasing the supposed redundant information. The present method tries to keep the original information by reducing the roles of pre-training as much as possible. All important precedences of potentiality assimilation are implemented in the main-training. As several reports stated, deep neural networks could produce better results without pre-training [25]. Our method to focus on the main learning is quite well suited for this situation.

B. Direct Potentiality Assimilation

In Figure 1, a neural network architecture with four hidden layers is shown in which the connection weights from the input to the first hidden layer for the pre-training are represented by $w_{j_1 j_0}^{(0)}$ with J_1 and J_0 neurons in the pre-training. Then, the positive weights are computed by

$$u_{j_1 j_0}^{(0)} = \max(w_{j_1 j_0}^{(0)}, 0). \quad (1)$$

By normalizing these weights, we have the potentiality

$${}^r \phi_{j_1 j_0}^{(0)} = \left(\frac{u_{j_1 j_0}^{(0)}}{u_{\max}^{(0)}} \right)^r, \quad (2)$$

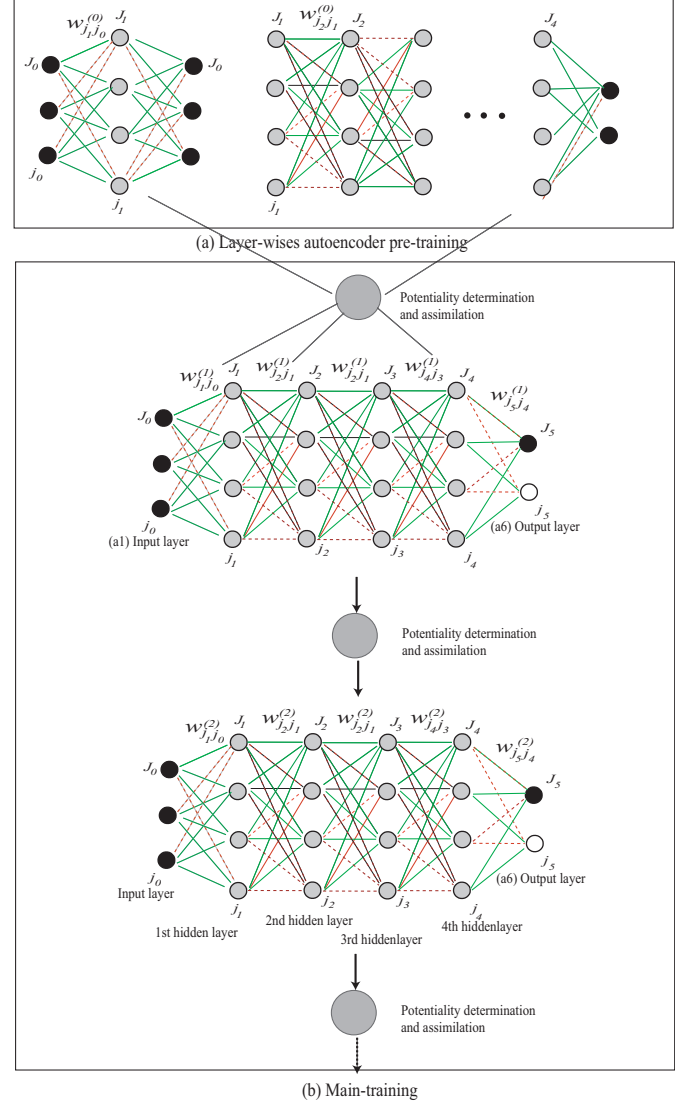


Fig. 1. Network architecture with four hidden layers by the direct potentiality assimilation.

where $u_{\max}^{(0)}$ denotes the maximum positive weight and r denotes the potential parameter. Using this potentiality, the selective potentiality can be defined by

$$\phi_{j_1 j_0}^r = \frac{J_1 J_0 - \sum_{j_1=1}^{J_1} \sum_{j_0=1}^{J_0} r \phi_{j_1 j_0}^{(0)}}{J_1 J_0 - 1}. \quad (3)$$

When all connection weights become zero, the selective potentiality is also zero. This selective potentiality increases when the number of strong connection weights decreases. In the end, potentiality reaches its maximum of one when only one weight is the strongest, while all the others are forced to be zero.

This potentiality is assimilated in the main training as

$$w_{j_1 j_0}^{(1)} = {}^r \phi_{j_1 j_0} w_{j_1 j_0}^{(0)}. \quad (4)$$

In the same way, for the second step, we have

$$w_{j_1 j_0}^{(2)} = {}^r \phi_{j_1 j_0}^{(1)} w_{j_1 j_0}^{(1)}, \quad (5)$$

where $r\phi_{j_1j_0}^{(1)}$ denotes the potentiality at the first step of learning.

The Average potentiality is the average of all potentialities, in this case, five different potentialities for five layers,

$$\phi_{avg}^r = \frac{1}{5} \sum_{k=1}^5 \phi_{j_k, j_{k-1}}^r. \quad (6)$$

C. Collective Interpretation

We focus on the interpretation of input neurons or variables. Since it is impossible to interpret all the connection weights of all intermediate layers, we try to treat them collectively. Thus, the potentiality of the input-output connection weights is computed by summing all weights in the intermediate layers. The collective weights from the input to the output layer are computed by

$$u_{j_5j_0} = \sum_{j_4=1}^{J_4} \sum_{j_3=1}^{J_3} \sum_{j_2=1}^{J_2} \sum_{j_1=1}^{J_1} w_{j_5j_4} w_{j_4j_3} w_{j_3j_2} w_{j_2j_1} w_{j_1j_0}. \quad (7)$$

We use here raw connection weights to see detailed characteristics. However, since connection weights are forced to be positive, the final collective weights are not so different from those by the positive weights.

III. RESULTS AND DISCUSSION

A. Student Evaluation Data Set

1) *Experimental Outline*: The data set was composed of 5,820 class evaluation scores by the students from the machine learning database [26]. Of total 33 variables, 28 variables were extracted on the evaluation questions. Then, the variable No.9, related to the class satisfaction¹ was used for the targets representing the class satisfaction. The 70 percent of the data set was for training and the remaining one for evaluation. We used the Matlab neural network package with all default parameter values, because we focused on the easy reproduction of the present results.

2) *Selectivity and Generalization*: Figure 2 shows the average selectivity (a) and generalization errors (b). As can be seen in the figures, the selectivity increased gradually in Figure 2(a), and correspondingly, the generalization errors decreased to the minimum point when the parameter r was increased from 0 to 1.1. Then, the generalization errors did not decrease but fluctuated. These results show that the selectivity can be used to increase generalization performance by choosing appropriately the parameter r .

3) *Comparison of Connection Weights*: Figure 3 shows connection weights when the parameter r was zero. Connection weights were almost random and it was impossible to detect any regularity over connection weights. Figure 4 shows connection weights when the parameter r was 1.1, producing the best generalization performance. Though some minor negative connection weights were seen in the weights to

¹Actually, the variable No.9 means that the students enjoyed the class very much.

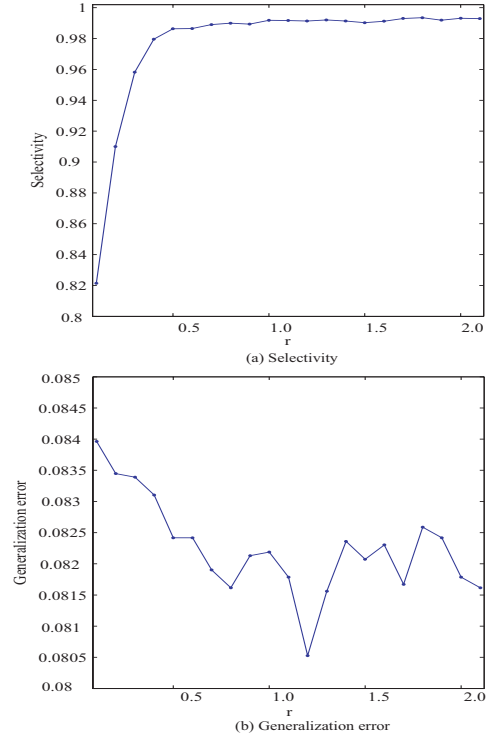


Fig. 2. Selectivity (a) and generalization errors (b) for the student evaluation data set.

the first hidden layer in Figure 4(a). The majority of weights were positive and they remained to be strong for all layers.

Let us examine why connection weights with $r=1.1$ in Figure 4 produced better generalization performance. In Figure 4, the vertical lines and horizontal lines were added. The horizontal lines represent that connection weights are connected with the subsequent connection weights. On the other hand, the vertical lines show that the corresponding weights are connected with ones located in the former layer. Connection weights to the fifth hidden neuron are strong in Figure 4(a) and they are connected with the third hidden neurons in the second hidden layer in Figure 4(b). Then, these neurons were connected with the fourth hidden neurons in Figure 4(c). Finally, the connection weights are connected with connection weights into the first output neuron in Figure 4(d). Thus, those connection weights make it possible to transmit information on original input patterns to the output layer.

4) *Interpreting Input Selective Potentiality*: Figure 5(a) shows the collective weights when the parameter was 1.1, giving the best generalization performance. As can be seen in the figures, the ninth input neuron took the highest weight value. When the class expectation is met by students, they tend to be satisfied with the class. On the other hand, Figure 5(b) show the regression coefficients by the logistic regression analysis. We can see the same tendency that the ninth variable had the largest value. However, some other variables had relatively larger values, for example, the variable No.16. These result show that the direct potentiality assimilation can extract clearer characteristics than logistic regression analysis. This is

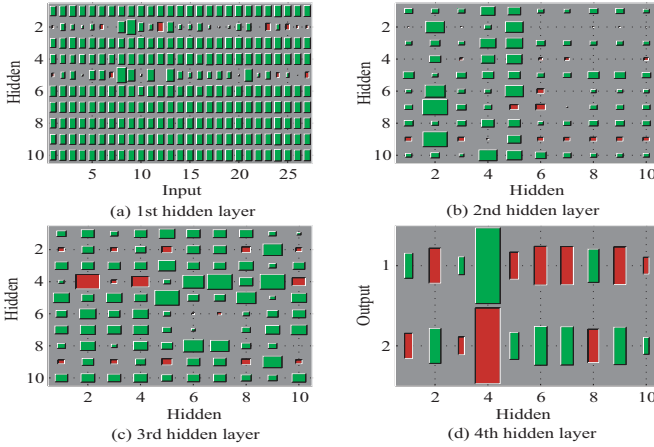


Fig. 3. Connection weights from the first (a) to output (d) layer when the parameter r was 0 for the student evaluation data set.

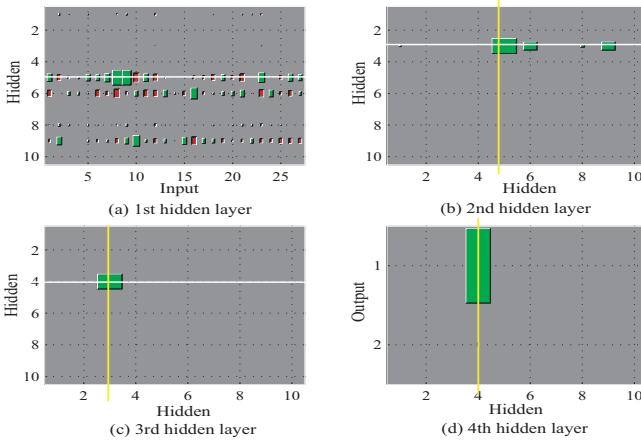


Fig. 4. Connection weights from the first (a) to output (d) layer with $r=1.1$ for the student evaluation data set.

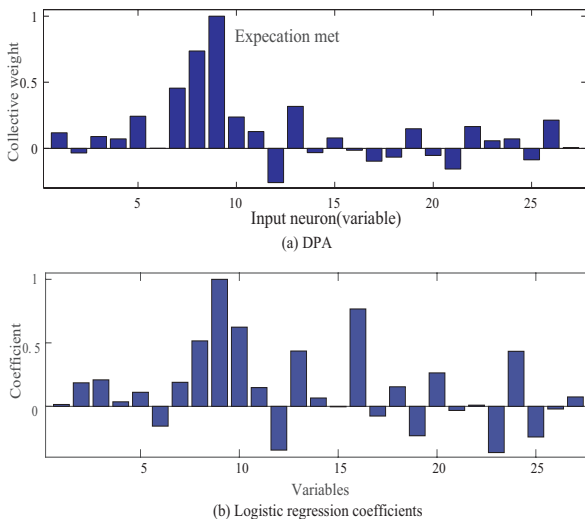


Fig. 5. Collective weights (a) and regression coefficients (b) by the logistic regression analysis.

due to the selective effect of potentiality assimilation.

5) *Generalization Comparison*: Table I shows the generalization performance by the logistic analysis, deep learning and direct potentiality assimilation method. The lowest errors were 0.0805, 0.0710 and 0.0899 in terms of average, minimum and maximum values when the parameter r was 1.1. The second best average error of 0.0868 was obtained by the logistic regression analysis. Then, the worst error of 0.0940 was by the deep learning with three hidden layers. This means that it became impossible to learn input patterns by the ordinary deep learning with auto-encoders. The unsupervised learning such as auto-encoders tends to lose information content gradually when the layer becomes higher.

IV. CONCLUSION

In the present paper, we proposed a new potential learning method in which the potentiality assimilation is transferred from the pre-training to the main-training. The potential learning has been originally developed to simplify complicated information-theoretic methods [11], [14]. Because of the complexity in computing entropy or mutual information, the methods have not been fully explored in the neural networks. In this context, the potential learning has been introduced to simplify the computational procedures of information maximization [8], [27], [9], [10]. First, the potentiality of some components is determined and then this potentiality is assimilated. Usually, a smaller number of components with higher potentiality is extracted. The potential learning has been applied to single-layered neural networks as well as multi-layered neural networks. To train the deep neural networks, the pre-training has been believed to have much importance. In multi-layered neural networks, the un-supervised pre-training is usually used to solve the vanishing information problem, inherent to the gradient descent. In addition, several regularization terms such as weight decay and sparsity constraints are implemented. These methods such as un-supervised pre-training with the regularization terms tend naturally to reduce information content on original input patterns. Actually, it is difficult to control information in the pre-training for the benefit of the subsequent main training. To solve this problem, though the pre-training is necessary in training multi-layered neural networks, the roles of the pre-training should be minimized. We think that the main role of pre-training is to give the overall or rough information content to be used in the main-training.

The method was applied to the student evaluation data set. Then, it could be observed that generalization performance could be improved. The final collective weights were very similar to those by the regression coefficients by the logistic regression analysis. This means that the present method extracted the same characteristics by the logistic regression analysis, taking into account some additional features which the conventional logistic analysis could not deal with.

The problem is that the potentiality was applied independently in all layers. This means that when the parameter was increased, and the effect of potentiality is more apparent, the potentiality tends to be assimilated independently in each layer. Finally, the layers tend to be dis-connected with each other.

TABLE I
SUMMARY OF EXPERIMENTAL RESULTS ON GENERALIZATION PERFORMANCE FOR THE STUDENT DATA SET.

Method	Layers	r	Avg	Std	Min	Max
Logistic			0.0868	0.0065	0.0733	0.0956
Deep	3		0.0940	0.0088	0.0762	0.1031
DPA		1.1	0.0805	0.0065	0.0710	0.0899

Then, it can be considered that the original information content in input patterns cannot be transmitted through layer. Thus, the information on input patterns tends to be lost gradually in the course of learning. To solve this problem, the present method should be formulated, taking into account the connectivity between neurons and layers. Though some problems should be solved for the practical data sets, the method is simple enough to be implemented in large-scale networks.

REFERENCES

- [1] R. Andrews, J. Diederich, and A. B. Tickle, "Survey and critique of techniques for extracting rules from trained artificial neural networks," *Knowledge-based systems*, vol. 8, no. 6, pp. 373–389, 1995.
- [2] J. M. Benítez, J. L. Castro, and I. Requena, "Are artificial neural networks black boxes?," *IEEE Transactions on neural networks*, vol. 8, no. 5, pp. 1156–1164, 1997.
- [3] M. Ishikawa, "Rule extraction by successive regularization," *Neural Networks*, vol. 13, no. 10, pp. 1171–1183, 2000.
- [4] T. Q. Huynh and J. A. Reggia, "Guiding hidden layer representations for improved rule extraction from neural networks," *IEEE Transactions on Neural Networks*, vol. 22, no. 2, pp. 264–275, 2011.
- [5] B. Mak and T. Munakata, "Rule extraction from expert heuristics: a comparative study of rough sets with neural network and ID3," *European journal of operational research*, vol. 136, pp. 212–229, 2002.
- [6] J. Yosinski, J. Clune, A. Nguyen, T. Fuchs, and H. Lipson, "Understanding neural networks through deep visualization," *arXiv preprint arXiv:1506.06579*, 2015.
- [7] D. Erhan, Y. Bengio, A. Courville, and P. Vincent, "Visualizing higher-layer features of a deep network," *University of Montreal*, vol. 1341, 2009.
- [8] R. Kamimura, "Simple and stable internal representation by potential mutual information maximization," in *International Conference on Engineering Applications of Neural Networks*, pp. 309–316, Springer, 2016.
- [9] R. Kamimura, "Collective interpretation and potential joint information maximization," in *Intelligent Information Processing VIII: 9th IFIP TC 12 International Conference, IIP 2016, Melbourne, VIC, Australia, November 18-21, 2016, Proceedings*, pp. 12–21, Springer, 2016.
- [10] R. Kamimura, "Repeated potentiality assimilation: Simplifying learning procedures by positive, independent and indirect operation for improving generalization and interpretation (in press)," in *Proc. of IJCNN-2016*, (Vancouver), 2016.
- [11] R. Linsker, "Self-organization in a perceptual network," *Computer*, vol. 21, no. 3, pp. 105–117, 1988.
- [12] R. Linsker, "How to generate ordered maps by maximizing the mutual information between input and output signals," *Neural computation*, vol. 1, no. 3, pp. 402–411, 1989.
- [13] R. Linsker, "Local synaptic learning rules suffice to maximize mutual information in a linear network," *Neural Computation*, vol. 4, no. 5, pp. 691–702, 1992.
- [14] R. Linsker, "Improved local learning rule for information maximization and related applications," *Neural networks*, vol. 18, no. 3, pp. 261–265, 2005.
- [15] G. Castellano and A. M. Fanelli, "Variable selection using neural-network models," *Neurocomputing*, vol. 31, pp. 1–13, 1999.
- [16] G. G. Oliveira, O. C. Pedrollo, and N. M. Castro, "Simplifying artificial neural network models of river basin behaviour by an automated procedure for input variable selection," *Engineering Applications of Artificial Intelligence*, vol. 40, pp. 47–61, 2015.
- [17] J. D. Olden, M. K. Joy, and R. G. Death, "An accurate comparison of methods for quantifying variable importance in artificial neural networks using simulated data," *Ecological Modelling*, vol. 178, no. 3, pp. 389–397, 2004.
- [18] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 1, pp. 3–55, 2001.
- [19] C. E. Shannon, "Prediction and entropy of printed english," *Bell system technical journal*, vol. 30, no. 1, pp. 50–64, 1951.
- [20] N. Abramson, "Information theory and coding," 1963.
- [21] G. Hinton, "A practical guide to training restricted boltzmann machines," *Momentum*, vol. 9, no. 1, p. 926, 2010.
- [22] J. Kim, V. D. Calhoun, E. Shim, and J.-H. Lee, "Deep neural network with weight sparsity control and pre-training extracts hierarchical features and enhances classification performance: Evidence from whole-brain resting-state functional connectivity patterns of schizophrenia," *NeuroImage*, vol. 124, pp. 127–146, 2016.
- [23] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, "Dropout: A simple way to prevent neural networks from over-fitting," *The Journal of Machine Learning Research*, vol. 15, no. 1, pp. 1929–1958, 2014.
- [24] T. Xiao, H. Li, W. Ouyang, and X. Wang, "Learning deep feature representations with domain guided dropout for person re-identification," *arXiv preprint arXiv:1604.07528*, 2016.
- [25] J. Schmidhuber, "Deep learning in neural networks: An overview," *Neural Networks*, vol. 61, pp. 85–117, 2015.
- [26] K. Bache and M. Lichman, "UCI machine learning repository," 2013.
- [27] R. Kamimura, "Self-organizing selective potentiality learning to detect important input neurons," in *Systems, Man, and Cybernetics (SMC), 2015 IEEE International Conference on*, pp. 1619–1626, IEEE, 2015.
- [28] D. C. Ciresan, U. Meier, L. M. Gambardella, and J. Schmidhuber, "Deep, big, simple neural nets for handwritten digit recognition," *Neural computation*, vol. 22, no. 12, pp. 3207–3220, 2010.

Concepts Ontology Algebras and Role Descriptions

Cyrus F Nourani*
Akdmkrd AI Research Affiliate
TU Berlin, Germany
Acdmkrd@gmail.com &
cyrusfn@alum.mit.edu

Patrik Eklund
Umeå University,
Department of Computing Science
Umeå, Sweden
peklund@cs.uum.se

Abstract—A heterogeneous computing model with ontology preserving functions are applied to present concept learning across domains with structural agent morphisms. A computing models based on a novel multi-agent competitive learning with multiplayer game tree plans are applied. Agents are assigned to transform the models to reach goal plans. Goals are satisfied based on competitive game tree learning. Agent tree computing models are example prototypes for modeling ontology algebras. Specific agents are assigned to transform the models to reach goal plans where goals are satisfied based on competitive game tree learning. Cooperating agents, that have opened new avenues in modeling and implementing agent teams, are ingredients to specific application modeling. Applications to Formal Concept Description are developed with new description logic algebraic models. Novel Description algebras with concept description ontology algebras and description ontology preservation morphisms are presented.

Index Terms—Game Learning Ontology Algebras, Description Ontology, Ontology Preservation Morphisms, Competitive Model Ontology, Agent Ontology Models, Game Tree Learning.

I. DESIRE MODELS

AN OVERVIEW to a practical agent learning based on new competitive modeling a technique applying what the first author developed since 2004 is presented with augmentation to standard agent modeling [11]. A specific agent might have internal state set I , which the agent can distinguish its membership. The agent can transit from each internal state to another in a single step. With our multi-board model agent actions are based on I and board observations. Transfer learning is carried on with agent morphisms. Predictive and competitive model learning is presented applying agent game trees. Ontology preservation principles are introduced for learning ontology. The preservation principles are further applied to the knowledge bases that support the transfer learning. Competitive game tree learning is the basis to the authors' application to business and economics game modeling. Deduction models attain a new perspective with the techniques here. Context abstraction and met-contextual reasoning is introduced as a new field. Multi-agent visual multi-board planning has been applied in the first author's

projects to space navigation and spatial computing learning. In a haptic computing logic [8] the learning process can be seen as an emotional and personal, game based, and proactive Game-based Learning, emotions and emotional agents, henceforth abbreviated as the BID model [16].

The section overviews are as follows. Section two develops the stage for the agent computing models that are applied to characterize agent computations based on standard Desire modeling augmented with newer agent module algebras. Section 3 presents the competitive modeling techniques with signed trees. Tree computations to realize goals for competitive models are the bases for model compatibility characterizations on realizing goals on computation trees. Generic model diagrams are applied to compare models. Section 4 presents signed tree morphisms and module preservation techniques based on alternative agent computing techniques. Agent algebras and morphisms render a basis for defining ontology preservation principles. Section 5 applies the techniques to model-based concept learning with preservation morphism mappings for transfer learning across domains. Section 6 develops the new basis for ontology algebras on Concept Descriptions. A categorical characterization encompasses a constructive description logic with concept description algebra monads on agent signature trees. Based on that new concept ontology algebras with description ontology algebra preservation theorem are presented. Newer application areas that can be explored are mutual robot learning – a robot introducing a structure to a new robot. These areas have started being explored at Singularity university affiliate groups, for example. Robot learning based on watching the task being performed by a human or by a second robot are model-based learning but troublesome due to a mismatch between the model structure problems e.g. [21]. Newer examples are on learning topological spaces [20]. Our more functional approach to learning about the world can be applied to physical robots transformed into an abstract model, and then converting it back into a functional representation.

II. DESIRE MODELS

Let us start with the popular agent computing model the Beliefs, Desire, and Intentions, BID is a generic agent computing model specified within the declarative compositional modeling framework for multi-agent systems, DESIRE. The model, a refinement of a generic agent model, explicitly specifies motivational attitudes and the static and dynamic relations between motivational attitudes. Desires, goals, intentions, commitments, plans, and their relations are modeled [6]. Different notions of strong and weak agency are presented at [22]. To apply agent computing with intelligent multimedia some specific roles and models have to be presented for agents. Beliefs, intentions, and commitments play a crucial role in determining how rational agents will act. Beliefs, capabilities, choices, and commitments are the parameters making component agents specific. DESIRE is the framework for design, and the specification of interacting reasoning components is a framework for modeling, specifying and implementing multi-agent systems, see [6], [22]. The interaction between components, and between components and the external world is explicitly specified. Components can be primitive reasoning components using a knowledge base, but may also be subsystems that are capable of performing tasks using methods as diverse as decision theory, neural networks, and genetic algorithms.

A. Specifying BID Agents

The BID design specifications in our papers apply agent signature trees. Information is encoded with a predicate logic on a hierarchically ordered sort structure (order-sorted predicate logic). Newer techniques with levels of signatures [17], [8] can be applied to the encoding. Units of information including sorts and operators of different arities are represented on the signature on the first level. On the second level, operators are type constructors, so that the set of variable-free terms are shifted down to the sort set for the signature on level three. In this way, different (meta)levels may be distinguished and richer type constructions can be obtained and used. Some specifics and a mathematical basis to such models with agent signatures might be obtained from [1] where the notion had been introduced since 1994. Meta-level information contains information about object-level information and reasoning processes; for example, for which atoms the values are still unknown (epistemic information). Similarly, tasks that include reasoning about other tasks are modeled as meta-level tasks with respect to object-level tasks.

III. COMPETITIVE MODELS AND SIGNATURED TREES

Planning is based on goal satisfaction at models. Multi-agent planning, in this paper is modeled as a competitive learning problem where the agents compete on game trees as candidates to satisfy goals hence realizing specific models where the plan goals are satisfied. When a specific agent group “wins” to satisfy a goal the group has presented a model to the specific goal, presumably consistent with an intended world model. For example, if there is a goal to put a spacecraft at a specific

planet’s orbit, there might be competing agents with alternate micro-plans to accomplish the goal [4]. While the galaxy model is the same, the specific virtual worlds where a plan is carried out to accomplish a real goal at the galaxy via agents are not. The plan goal selections and objectives are facilitated with competitive agent learning. The intelligent languages [15] are ways to encode plans with agents and compare models on goal satisfaction to examine and predict via model diagrams why one plan or model is better than another or to prevent traversing unsuccessful routes.

B. Intelligent AND/OR Trees and Search

AND/OR trees Nilsson e.g. [23] are game trees defined to solve a game from a player's stand point.

Formally a node problem is said to be solved if one of the following conditions hold.

1. The node is the set of terminal nodes (primitive problem – the node has no successor).
2. The node has AND nodes as successors and the successors are solved.
3. The node has OR nodes as successors and any one of the successors is solved.

A solution to the original problem is given by the subgraph of AND/OR graph sufficient to show that the node is solved. A program which can play a theoretically perfect game would have task like searching and AND/OR tree for a solution to a one-person problem to a two-person game. An agent AND/OR tree [1] is an AND/OR tree where the tree branches are intelligent trees. The branches compute a Boolean function via agents. The Boolean function is what might satisfy a goal formula on the tree. An intelligent AND/OR tree is solved iff the corresponding Boolean functions solve the AND/OR trees named by agent functions on the trees. Thus node m might be $f(a_1, a_2, a_3) \& g(b_1, b_2)$, where f and g are Boolean functions of three and two variables, respectively, and a_i 's and b_i 's are Boolean valued agents satisfying goal formulas for f and g . An intelligent AND/OR tree is solved iff the corresponding Boolean functions solve the AND/OR trees named by intelligent functions on the trees. Thus node m might be $f(a_1, a_2, a_3) \& g(b_1, b_2)$, where f and g are Boolean functions of three and two variables, respectively, and a_i 's and b_i 's are Boolean valued agents satisfying goal formulas for f and g .

A tree game degree is the game state a tree is at with respect to a model truth assignment, e.g. to the parameters to the Boolean functions above. Let generic diagram or G-diagrams be diagrams definable by specific functions. Intelligent signatures [1] are signatures with designated multiplayer game tree function symbols. A soundness and completeness theorem is proved on the intelligent signature language by the first author [7]. The techniques allowed us to present a novel model-theoretic basis to game trees, and generally to the new intelligent game trees.

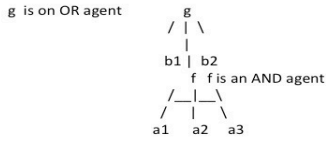


Figure 1: Agent Logic Tree

C. Trees and Model Compatibility

Now let us examine the definition of situations from 1985 times and view it in the present formulation.

Definition 3.1 A situation consists of a nonempty set D , the domain of the situation, and two mappings: g, h . g is a mapping of function letters into functions over the domain as in standard model theory. h maps each predicate letter, pn , to a function from D^n to a subset of $\{t, f\}$, to determine the truth value of atomic formulas as defined below. The logic has four truth values: the set of subsets of $\{t, f\}$, $\{\{t\}, \{f\}, \{t, f\}, 0\}$. the latter two is corresponding to inconsistency, and lack of knowledge of whether it is true or false.

The above truth value assignments indicate that the number of situations exceeds the number of possible worlds. The possible worlds being those situations with no missing information and no contradictions. From the above definitions the mapping of terms and predicate models extend as in standard model theory. Next, a compatible set of situations is a set of situations with the same domain and the same mapping of function letters to functions. In other worlds, the situations in a compatible set of situations differ only on the truth conditions they assign to predicate letters.

Definition 3.2 Let M be a structure for a language L , call a subset X of M a generating set for M if no proper substructure of M contains X , i.e. if M is the closure of $X \cup \{c_M : \text{for } c, \text{ a constant symbol of } L\}$. An assignment of constants to M is a pair $\langle A, G \rangle$, where A is an infinite set of constant symbols in L and $G: A \rightarrow M$, such that $\{G[a] : a \in A\}$ is a set of generators for M . Interpreting a by $G[a]$, every element of M is denoted by at least one closed term of $L[A]$. For a fixed assignment $\langle A, G \rangle$ of constants to M , the diagram of M , $D\langle A, G \rangle[M]$ is the set of basic [atomic and negated atomic] sentences of $L[A]$ true in M . [Note that $L[A]$ is L enriched with set A of constant symbols.]

Generic diagrams, denoted by G -diagrams, were what we defined since 1980's to be diagrams for models defined by a specific function set, for example Σ_1 Skolem functions.

Remark: The functions above are those by which a standard model could be defined by inductive definitions.

The first author proved [5] that situations are compatible iff their corresponding generalized diagrams are compatible with respect to the Boolean structure of the set to which formulas are mapped (by the function h above, defining situations). To examine compatibility on model diagrams minimal prediction was developed around 1994. The artificial intelligence technique defined since the author's model-theoretic planning project, is a cumulative nonmonotonic approximation attained with completing model diagrams on what might be true in a model or knowledge base. The predictive diagrams [9] are applied to discover models to the intelligent game trees. Prediction is applied to plan goal satisfiability and can be combined with plausibility [5] probabilities, and fuzzy logic, e.g. [13], [17] to obtain, for example, confidence intervals.

IV. SIGNATURED MORPHISMS AND MODULE PRESERVATION

From the software agent designer's viewpoint, however, there is modularity with artificial structures. Artificial structures [7] implemented by agent morphisms. Knowledge acquisition requires either interviewing an expert, brainstorming with a group of experts, or structuring one's thoughts if the specifier is the expert. For multi-agent designs there are active learning agents and automatic learning. The author first author had presented the notion of Nondeterministic Knowledge (Design_Agents) [7]. Design_Agents is formulated to deal with the conceptualization stage and is being applied by the present project to define active learning by agents.

Design_Agents requires the user to inform the specifier as to the domains that are to be expected, i.e. what objects there are and what the intended actions (operations) on the objects are, while fully defining such actions and operations. The actions could be in form of processes in a system. The relations amongst the objects and the operations (actions) can be expressed by algebras and clauses, which the specifier has to present. The usual view of a multi-agent systems might convey to an innocent AI designer that an agent has a local view of the environment, interacts with others and has generally partial beliefs (perhaps erroneous) about other agents. On the surface the Design_Agents specification techniques might appear as being rigid as to what the agents expect from other agents. The Design_Agents specification does not ask the agents be specified up to their learning and interaction potential. Design_Agents only defines what objects might be involved and what might start off an agent. It might further define what agents are functioning together. Thus specifications are triples $\langle O, A, R \rangle$ consisting of objects, actions and relations. Actions are operations or processes.

A. The Formal Basis

Starting with what are called hysteretic agents [11]. A hysteretic agent has an internal state set I , which the agent can distinguish its membership. The agent can transit from each internal state to another in a single step. Actions by agents are

based on I and board observations. There is an external state set S, modulated to a set T of distinguishable subsets from the observation viewpoint. An agent cannot distinguish states in the same partition defined by a congruence relation. A sensory function $s : S \rightarrow T$ maps each state to the partition it belongs. Let A be a set of actions which can be performed by agents. A function action can be defined to characterize an agent activity $\text{action} : T \rightarrow A$. There is also a memory update function $\text{mem} : I \times T \rightarrow I$. To define agent at arbitrary level of activity knowledge level agents are defined. All excess level detail is eliminated. In this abstraction an agent's internal state consists entirely of a database of sentences and the agent's actions are viewed as inferences based on its database. The action function for a knowledge level agent maps a database and a state partition t into the action to be performed by an agent in a state with database and observed state partition t. $\text{action} : D \times T \rightarrow A$. The update function database maps a state and a state partition t into a new internal database. $\text{database} : D \times T \rightarrow D$. A knowledge-level agent in an environment is an 8-tuple shown below. The set D in the tuple is an arbitrary set of predicate calculus databases, S is a set of external states, T is the set of partitions of S, A is a set of actions, see is a function from S into T, do is a function from A S into S, database is a function from D x T into D, and action is a function from D x T into A.

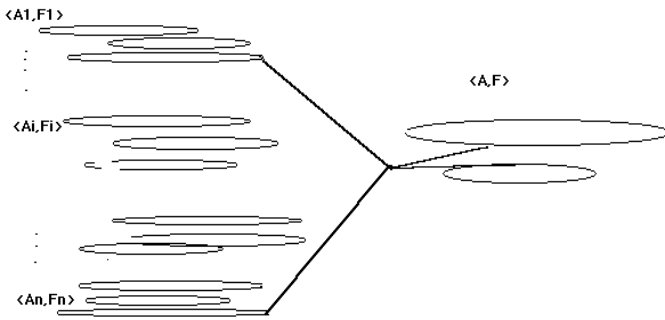


Figure 2 Heterogenous Module Computing Model

B. Agent Model Morphisms

Let A be a set of actions which can be performed by agents. A function action can be defined to characterize an agent activity $\text{action} : T \rightarrow A$. There is also a memory update function. A hysterectic agent HA defined by a sextuple $\langle I, S, T, A, s, d, \text{internal}, \text{action} \rangle$ where d is a function form $A \times S \rightarrow S$ and internal $I \times T \rightarrow I$. Let HA be a set of sextuples defining a hysterectic agents. Define HA morphims by a family of functions defined component-wise on the sextuple above.

Definition 4.1 A HA morphism is a function $F : HA \rightarrow HA'$ defined component-wise by $F[i] : I \rightarrow I'$; $F[S] : S \rightarrow S'$, $F[T] : T \rightarrow T'$, $F[A] : A \rightarrow A'$; $F[s] : S \rightarrow T'$; $F[d] : A' \times S' \rightarrow S'$ and $F[\text{internal}] : I' \times T' \rightarrow I'$.

Definition 4.1 implies F defines a new hysterectic agents from HA by a morphism. Component-wise definitions for a morphism might be viewed as functions on a multi-sorted

signature carrying the sextuple. Similar morphisms can be defined for knowledge level agents which we can refer to by KD-morphisms.

C. Agents, Modules, and Algebras

The computing enterprise requires more general techniques of model construction and extension, since it has to accommodate dynamically changing world descriptions and theories. The models to be defined are for complex computing phenomena, for which we define generalized diagrams. They were designed to build models with prespecified generalized Skolem functions. The specific minimal set of function symbols is the set with which a model fro a knowledge base can be defined. The G-diagram techniques allowed us to formulate AI worlds, KB's in a minimal computable manner to be applied to agent computation. The techniques in [5] for model building as applied to the problem of AI reasoning allow us to build and extend models through diagrams. A technical example of algebraic models defined from syntax had appeared in defining initial Σ algebras for equational theories of data types [2] and our research in [1]. In such direction for computing models of equational theories of computing problems are presented by a pair (Σ, E) , where Σ is a signature (of many sorts, for a sort set S and E a set of -equations.

Definition 4.2 An s-sorted signature Σ or operator domain is a family $\langle w, s \rangle$ of sets, f or s S and w S^* (where S^* is the set of all finite strings from S, including the empty string). call f $\langle w, s \rangle$ and operation symbol of rank w, s; of arity w, and of sort s. #

We apply multi-sorted algebras via Definition 2.3 to multi-agent systems.

Definition 4.3 Let Σ be an S-sorted signatures. A Σ -algebra A consists of a set A_s for each s S (called the carrier if A of sort s) and a function $\langle A \rangle : A_{s_1} \times A_{s_2} \times \dots \times A_{s_n} \rightarrow A_s$ for each $\langle w, s \rangle$, with $w = s_1 s_2 \dots s_n$ (called the operation named by $\langle w, s \rangle$). For $\langle s, s \rangle$, A_s , i.e the (set of names) of constants of sort s. #

Definition 4.4 If A and B are Σ algebras, a Σ -homomorphism $h : A \rightarrow B$ is a family of functions $\langle h_s : A_s \rightarrow B_s \rangle_{s \in S}$ that preserve the operations, i.e. that satisfy (h0) For $\langle w, s \rangle$, the $h_s(A) = B$; (h1) If $\langle w, s \rangle$, with $w = s_1 s_2 \dots s_n$ and $\langle a_1, \dots, a_n \rangle \in A_{s_1} \times A_{s_2} \times \dots \times A_{s_n}$, then $h_s[A(a_1, \dots, a_n)] = B(h_{s_1}(a_1), \dots, h_{s_n}(a_n))$.

From [1], [7] we have the following notions:

Definition 4.5 A signature is intelligent iff it has intelligent function symbols. We say that a language has intelligent syntax if the syntax is defined on an intelligent signature.

Definition 4.6 A language L is said to be an intelligent language iff L is defined from an intelligent syntax.

A practical example of intelligent languages was presented composed from $\langle O, A, R \rangle$ triples as control structures, e.g. SERF [15]. The functions in AF are the agent functions

capable of message passing. The O refers to the set of objects and R the relations defining the effect of A 's on objects. Amongst the functions in AF only some interact by message passing. The functions could affect objects in ways that affect the information content of a tree. There you are: the tree congruence definition thus is more complex for intelligent languages than those of ordinary syntax trees. Let us define tree information content for the present formulation. Hence there is a new frontier for a theoretical development of the $\langle O, A, R \rangle$ algebras and that of the AII theory. $\langle O, A, R \rangle$ is a pair of algebras, $\langle Alg[A], Alg[F] \rangle$, connected by message passing and AII defines techniques for implementing such systems. To define AII we define homomorphisms on intelligent signature algebras. For an intelligent signature $\mathcal{I}\Sigma$, let $T_{\mathcal{I}\Sigma}$ be the free tree word algebra of signature $\mathcal{I}\Sigma$. The quotient of $T_{\mathcal{I}\Sigma}$ the word algebra of signature $\mathcal{I}\Sigma$, with respect to the I -congruence relation generated by a set of equations E , will be denoted by $T\langle \mathcal{I}\Sigma, E \rangle$, or $T\langle P \rangle$ for presentation Component-wise definitions for a morphism might be viewed as functions on a multi-sorted signature carrying the sextuple. Similar morphisms can be defined for knowledge level agents which we can refer to by KD-morphisms. The techniques in [5] for model building as applied to the problem of AI reasoning allows us to build and extend models through diagrams. The notion of an intelligent signature [1] is simply a designation that there is a subsignature with specific properties, for example all the functions are 1-1.

Definition 4.7 A $\mathcal{I}\Sigma$ -homomorphism is a I -homomorphism defined on algebras with intelligent signature $\mathcal{I}\Sigma$. To define agent specific designs we apply HA-morphisms via the following definition.

Definition 4.8 Let A and B be $\mathcal{I}\Sigma$ -algebras with signatures containing an agent signature HA .

A HA-homomorphism from A to B is an $\mathcal{I}\Sigma$ -homomorphism with defined HA-morphism properties.

V. LEARNING, CONCEPTS, AND ONTOLOGY PRESERVATION

Our transfer learning model applies the BID model to specify learning areans $M1$ and $M2$. Each arean's BID is presented with intelligent signatures $\mathcal{I}\Sigma 1$ and $\mathcal{I}\Sigma 2$. Predictive model compatibility techniques are presented with agent signature game trees where the above formalism can be applied to realize competitive learning models. The following process is applied to transfer game tree and competitive model learning across domains since modeling and realizability are based on morphism preserved formulas.

The term ATL here refers to the process of abstract transfer learning from an abstract characterization of a world, or learning domain to a second arena or world. Thus ATL express the relationship between two forms of representations. The notion of abstract transfer learning are either algebraic or model-theoretic (algebraic logic) definitions. We refer to specifications of the form $\langle O, A, R \rangle$ as presentations that present an IM_BID system. We also expect a presentation of the form $\langle I[O], I[A], I[R] \rangle$ [15] for the implementing abstract or

concrete machine. The former could be the designer's conceptualization, and the latter the specification of the syntax and semantics of a programming language. Informally the ATL process is that of encoding the algebraic structure of the conceptualization of a problem onto the algebra that specified an learning machine, or a secondary BID specified world. The ATL process becomes that of defining specific agent and structural morphisms on the above BID algebras. Each of the functions defined by $\langle O, A, R \rangle$ are implemented by agents, that characterize the implementation function

$I: \langle O, A, R \rangle \rightarrow \langle I[O], I[A], I[R] \rangle$ is to be defining a mapping $I: \langle Alg[A], Alg[F] \rangle \rightarrow \langle Alg[I(A)], Alg[I(F)] \rangle$. We refer to $Alg[A]$ and $Alg[F]$ are what we call ontology algebras. The implementation mapping I defines wrappers to resources in a manner preserving the ontology algebra. Ontology algebras are multi-sorted algebras defining multi-agent systems defined by formal agents, e.g., hysterectic or knowledge level agents and agent morphisms [14], [15].

Example 1: Data and Knowledge Bases: The ATL Ontology Preservation Principle, following is the first author's 1997 ontology preservation principles: The ATL is a valid transfer only if it preserves the ontology algebras. Since the knowledge-base is essential to learning designs, let us carry on the ontology preservations to Widerhold's domain knowledge base algebra DKB [16] consists of matching rules linking domain ontologies. There are three operations defined for DKB .

Example 2: Mutual Robot Learning

Based on that new concept ontology algebras with description ontology algebra preservation theorem are presented. Newer application areas that can be explored are mutual robot learning – a robot introducing a structure to a new robot. These areas have started being explored at Singularity university affiliate groups, for example. Newer examples are on learning topological spaces [20]. Our more functional approach to learning about the world can be applied to physical robots transformed into an abstract model, and then converting it back into a functional representation.

The operations are: Intersection – creating subset ontology and keeping sharable entries; Union – creating a joint ontology merging entries; Difference – creating a distinct ontology and removing shared entries. Mapping functions must be shown to preserve ontologies. Structural morphism allow ontology structures to be mapped from one robot ontology Knowledge base to a new robot with alternate ontology descriptions and structures, thereby transfer learning to a new robot with alternate ontology with structure preserving morphisms.

Based on that new concept ontology algebras with description ontology algebra preservation theorem are presented. Newer application areas that can be explored are mutual robot learning – a robot introducing a structure to a new robot. These areas have started being explored at Singularity university affiliate groups, for example. Robot learning based on watching the task being performed by a human or by a second robot are model-based learning but troublesome due to

a mismatch between the model structure problems e.g. [21]. Newer examples are on learning topological spaces [20]. Our more functional approach to learning about the world can be applied to physical robots transformed into an abstract model, and then converting it back into a functional representation. Let us apply the definition for HA agents and HA morphisms to state a preservation theorem. Let A and B be $\mathcal{I}\Sigma$ -algebras with the signature $\mathcal{I}\Sigma$ containing HA agents. Let $\text{Alg}[B]$ be an $\mathcal{I}\Sigma$ -algebra defined from B implementing, e.g. [15] a specified functionality defined by A . An ATL is an implementation for $\text{Alg}[A]$ by $\text{Alg}[B]$. Theorems 5.1 and 5.2 are from the first author's 2001 times, c.f. [15].

Definition 5.1 Let A and B be $\mathcal{I}\Sigma$ -algebras with intelligent signature $\mathcal{I}\Sigma$ containing agents. An I -ontology is an $\mathcal{I}\Sigma$ -algebra with axioms for the agents and functions on the signature.

Theorem 5.1 Let A and B be $\mathcal{I}\Sigma$ -algebras with the signature $\mathcal{I}\Sigma$ containing HA agents. The AII with HA morphisms defined from A to B preserve $\mathcal{I}\Sigma$ -ontology algebras iff defined by HA-homomorphisms.

Proof definition for the ontologies, HA morphism, definition 4.7 and 4.8, $\mathcal{I}\Sigma$ -algebras and $\mathcal{I}\Sigma$ -homomorphisms entail the $\mathcal{I}\Sigma$ -ontology axioms are preserved iff agents are carried by HA-homomorphisms from A to B .

Theorem 5.2 Let A and B be $\mathcal{I}\Sigma$ -algebras with the signature $\mathcal{I}\Sigma$ containing KD agents. The AII with KD morphisms preserve $\mathcal{I}\Sigma$ -ontology algebras iff defined by KD-homomorphisms.

Proof Similar to 5.1. DKB mappings are specific ATL's were the ontology algebra operations are the same at source and target. We can prove based on the above that DKB mappings are DKB preservation consistent.

VI. FORMAL CONCEPT DESCRIPTION ONTOLOGY ALGEBRA

FCA is abstracted on so called "context", or "formal context", but is in the end just a relation on sets, $I \subseteq G \times M$, often written as and said to be a triple (G, M, I) . G is called these to "objects" and M these to "attributes". However, neither objects nor attributes are given any specific syntactic structure. The call for intuitive meaning, but as such there is no syntactic structure [24,25] whatsoever based on which objects and attributes move beyond being just points in sets. This obviously makes real-world applications difficult to develop, and application content is all in that intuitive structure, and none of it is embraced by the syntactic notion itself. Basically, in FCA, G and M are indeed just plain sets, but in this starting point they can be seen as objects in the category Set of sets and functions. Further, even if in traditional FCA, the elements of those sets have no structure whatsoever, these sets can be provided with generalized structure [17], which formalizes FCA categorically, thereby opening up possibilities to give "object" and "attribute" more precise meanings given their syntactic structure, also going beyond just using Set as the underlying category for FCA, and, adopting a much more generalized view on relations.

In traditional FCA (Wille 1982), a so called "formal concept", or just a "concept", is a pair (A, B) , with $A \subseteq G$ and $B \subseteq M$, such that $A = \{g \in G \mid g \text{Im for all } m \in B\}$ and $B = \{m \in M \mid g \text{Im for all } g \in A\}$. A lattice, the so called "formal concept lattice", is given for the set of all concepts by $(A_1, B_1) \leq (A_2, B_2)$ if and only if $A_1 \subseteq A_2$ (or, equivalently, $B_1 \supseteq B_2$). Since there is no convention about how to use given names for objects and attributes in "informally constructed" names for formal concepts, combining names into names for concepts, or simply inventing the names otherwise, has become tradition within FCA. This, however, means that there is no terminological or ontology basis for FCA, but concepts themselves are seen as ontology objects. The ontology preservation areas will be further developed to present concept ontology mappings and preservations.

In the following subsection we show how constructive and type-theoretic methodology can provide enriched structures for FCA. The constructive approach Paive (2002) adapts classical ALC to a constructive system using the two routes outlined above. The syntax of such constructive system is the same in both cases. Concept descriptions in this constructive description logic CDL language obey the following syntax rule

$$C, D \rightarrow A \mid T \mid \perp \mid C \sqcap D \mid C \sqcup D \mid C \rightarrow D \mid \forall R.C \mid \exists R.C$$

where C, D range over concepts, A is an atomic concept and R ranges over names of roles, as before. As usual in constructive logics, since $\neg C$ is simply an abbreviation for $C \rightarrow \perp$ we do not need to consider it. In compensation we must add in the constructive implication of concepts, which in classical description logic is a derived concept. Also it is just a convenience to have the true concept T , as it could be defined as $\neg \perp$. We are then within the realm of first order logic IFOL.

The type-theoretic approach shows how concepts as singleton concepts correspond to "individual concept", whereas syntactic powers of concepts correspond to "concept".

A. Categorical Characterizations

In this subsection we point out that \exists in $\exists R.C$ as a modality is actually an informal symbol. Further, as typing comes into play, we show how C is syntactically ambiguous in this context as the underlying signature is not precisely described.

In the following we use notations from (Schmidt-SchaussSmolka 1991). Note that D for the universe should not be confused with D as used for concept descriptions, e.g., in expressions like $C \sqcup D$, D is not to be understood as D in D^I , where I is the interpretation. With C as a "concept", we have C^I as a subset of D^I , which in turn is an element $P D^I$, where P is the powerset functor. The "existential quantifier" in $\exists R.C$ is an "R-modality" applied to the powerconcept C .

The definition for the semantic expression $(\exists R.C)^1$ uses the existential quantifier that appears in the assumed underlying set theory. Concerning the underlying signature and related variables, in (Schmidt-SchaussSmolka1991) the situation is unclear, given the assumption about the existence of two further disjoint alphabets of symbols, which are called individual and concept variables. Logically, variables are not part of any alphabet. Variables are terms, and as such they are terms of a certain type. We should therefore speak of "individual concept" rather than "individual variable". Now typing of "concept" and "individual concept" comes into play, and we will need type constructors on level two of the so called three-level arrangement of signatures [17]. As opposed to (Schmidt-SchaussSmolka1991), we say "concept" instead of "individual concept", and "powerconcept" instead of "concept". The underlying signature must be formalized, where concept is a sort in the given underlying signature on level one. On level two, Pconcept becomes a constant operator, and a type constructor P is then used to produce a new type Pconcept, which in their 'algebra' will be understood, respectively, as D^1 and PD^1 . Simply typed description logic can now be formally defined in lambda-calculus [17]. A concept on level one becomes a "singleton powerconcept" on level three, and the syntactic expression $\exists R.C \text{ app}_{P(\text{Pconcept}), \text{Pconcept}}(m, \text{app}_{\text{Pconcept}, P(\text{Pconcept})}(R,C))$ where m is the multiplication of the underlying monad, and app is the function type constructor.

For transforming description logic into our categorical framework, we use notations in [6]. Interpretations $I = (D^1, I)$, where I maps every concept description to a subset of D^1 , use D for that universe, which should not be confused with D as used for concept descriptions, e.g., in expressions like $C D$, where D is not to be understood as the "D in D^1 ". With C as a "concept", we have $C^1 \subseteq D^1 \in P D^1$. This means that $P D^1$ is the actual 'algebra'. Roles R are semantically described as relations $RI \subseteq D^1 \rightarrow D^1$, i.e., we can equivalently write it as a substitution $R^1 : D^1 \rightarrow D^1$. The observation that relations $R \subseteq X \rightarrow X$ correspond precisely to functions (in form of substitutions) $R : X \rightarrow PX$, where P is the powerset functor over the category of sets and functions, is the basis for viewing generalized relations as morphisms (substitutions) in the Kleisli category over generalized powerset monads. With C as a "concept", we have $C^1 \subseteq D^1 \rightarrow PD^1$. This means that PD^1 is the actual 'algebra'.

Definition 6.1 A Description algebra morphism $h: PD^1 \rightarrow PD^1$ where I and I' are alternate interpretation functions such that h preserves roles R on D .

Following definitions on HA morphisms and the state space agent model above, we have description algebras defined on an agent signature Σ . Considering a sequence description competitive model [10] a concept interpretation I corresponds to a competitive model on an agent learning tree. Signed agent trees satisfy goals to complete a model diagram realizing a role R . Concept descriptions are presented with an agent signature tree T_E with a role R defined on the signature agents.

Proposition 6.1 A description algebra morphism on free signature tree $\wp(T_E)$ such that roles are preserved on T_E algebra is definable by algebraic extension on an agent signature algebra T_E .

Let us present the agent competitive instance for an algebraic description model platform.

Definition 6.2 Let A and B be description algebras with intelligent signature Σ containing agents. An Σ -ontology description is an Σ description algebra with a prescribed role $R: X \rightarrow \wp(\Sigma)$ for the agents and functions on the Σ signature.

Remark: $X \subseteq \Sigma$, so for a set monad, there is an assignment for all Σ well-formed trees. Example well-formed agent trees were presented in the first authors publications around 2007 on ISL algebras with 1-1 signature trees.

Theorem 6.1 Let A and B be Σ description algebras with the signature Σ . Then the agent homomorphisms defined from A to B preserve Σ -ontology iff defined by a description algebra homomorphisms by algebraic extension on free signature tree $\wp T_E$ such that roles are preserved on T_E .

Proof Theorems 5.1, 5.2, and Proposition 6.1.

Theorem 6.2 Let A and B be Σ -description algebras with the signature Σ containing KD agents. The AII with KD morphisms preserve Σ -description ontology algebras iff defined by KD-Description ontology homomorphisms.

Proof Similar to 6.1. DKB mappings are specific ATL's where the ontology algebra operations are the same at source and target. We can prove based on the above that DKB mappings are DKB preservation consistent.

VII. CONCLUDING COMMENTS

A sound computing basis for ontology structures descriptions, and preservation theorems are accomplished with ontology preserving functions and morphisms that are applied to transform learning across domains. Competitive learning models based on a novel multi-agent have increasing important applications ranging from structural learning to predictive data analytics based on goal plans. Roles and description are developed with new algebraic models with newer applications to concept description ontology algebras and description ontology preservation. The areas are a basis to future research on ontology structures with a comprehensive mathematical basis. Newer areas to explore are ATL principle for mutual robot learning based on ontology preservation morphisms.

ACKNOWLEDGMENTS

We thank our colleague Prof. Dominik Slezak, Warsaw University for his comments on the presentation.

* Sequent Description Logic computing was developed at Computation logic Lab., Burnaby, Canada: Akdmkrd.tri-pod.com

REFERENCES

- [1] Nourani, C. F. 1996, Slalom Tree Computing – A Computing Theory For Artificial Intelligence, June 1994 (Revised December 1994), A.I. Communication Volume 9, Number 4, December 1996, IOS Press, Amsterdam.
- [2] ADJ-Goguen, J.A., J.W. Thatcher, E.G. Wagner and J.B. Wright, A Junction Between Computer Science and Category Theory (parts I and II), IBM T.J. Watson Research Center, Yorktown Heights, N.Y . Research Report, 1975. 350.
- [3] Nourani, C. F. 2009, A Descriptive Computing, Information Forum, Leipzig, Germany, March 2009. SIWN2009 Program, 2009. The Foresight Academy of Technology Press International Transactions on Systems Science and Applications, Vol. 5, No. 1, June 2009, pp. 60-69. M. Wooldridge and N.R. Jennings, Intelligent Agents. (1993) 51- 92.
- [4] Koehler, J. 1986, Planning From Second Principles, AI 87.
- [5] Nourani, C. F. 1991, Planning and Plausible Reasoning in Artificial Intelligence, Diagrams, Planning, and Reasoning, Proc. Scandinavian Conference on Artificial Intelligence, Denmark, May 1991, IOS Press.
- [6] Brazier, F.M.T. Dunin-Keplicz, B., Jennings, N.R. and Treur, J. (1997) DESIRE: modelling multi-agent systems in a compositional formal framework, International Journal of Cooperative Information Systems, M. Huhns, M. Singh, (Eds.), special issue on Formal Methods in Cooperative Information Systems, vol. 1. Knowledge-based Systems workshop, KAW'95, Calgary: SRDG Publications, Department of Computer Science.
- [7] Nourani, C. F. 1995, Intelligent Languages - A Preliminary Syntactic Theory, May 15, 1995, Mathematical Foundations of Computer Science; 1998, 23rd International Symposium, Brno, Czech Republic, August The satellite workshop on Grammar systems. Silesian University, Faculty of Philosophy and Sciences, Institute of Computer Science, Science; 1450, Springer, 1998, ISBN 3-540- 64827-5, 846 pages.
- [8] Nourani, C. F. 2005, A Haptic Computing Logic – Agent Planning, Models, and Virtual Trees, 286-311., Affective And Emotional Aspects Of Human-Computer Interaction: Game-Based and Innovative Learning Approaches, Edited by Maja PIVEC, IOS PRES, 2006, pp. 317, ISBN1-58603-572-X.
- [9] Nourani, C. F. and T. Hoppe 1994, “GF-Diagrams for Models and Free Proof Trees,” Proceedings the Berlin Logic Colloquium, Universitat Potsdam, Organized by Humboldt Universitat Mathematics, Berlin. May 1994.
- [10] Cyrus F. Nourani and Oliver Schulte, Multiagent Decision Trees, Competitive Models, and Goal Satisfiability. DICTAP, Ostrava, Czech Republic, July 2013.
- [11] Genesereth, M. R. and N. J. Nilsson 1987, Logical Foundations of Artificial Intelligence, Morgan-Kaufmann, 1987.
- [12] Nourani, C. F. 2005, Agent-based Structures, Agent Ontology Preservation and Enterprise Modeling Workshop on Ontologies in Agent Systems 5th International Conference on Autonomous Agents Montreal, Canada.
- [13] U. Straccia, A fuzzy description logic, in: J. Mostow, C. Rich (Eds.), AAAI/IAAI, AAAI Press / The MIT Press, 1998, 594-599.
- [14] Nourani, C. F. “Design with Software Agents, Parallel Module Coordination and Object Languages, February 3, 1997. TU Berlin, Fachbereich 13 - Informatik, Sekretariat FR5-13, Berlin, Germany.
- [15] Nourani, C. F. “Abstract Implementation Techniques for A. I. By Computing Agents.: A Conceptual Overview,” Technical Report, March 3, 1993, Proceedings SERF-93, Orlando, Florida, November 1993. Published by the University of West Florida Software Engineering Research Forum, Melbourne, Florida.
- [16] Gio Wiederhold: “Interoperation, Mediation and Ontologies”; Proc.Int.Symp. on Fifth Generation Comp Systems, ICOT, Tokyo, Japan, V ol.W3, Dec.1994, pages 33-48.
- [17] Eklund, P., Galán, M. A., Kortelainen, J., Ojeda-Aciego, M. (2014). Monadic formal concept analysis, RSCTC 2014, (Eds. C. Cornelis et al.), Lecture Notes in Artificial Intelligence 8536, 201-210. pp. 473-484.
- [18] Eklund, P., Galán, M.A., Gahler, W.: Partially ordered monads for monadic topologies, Kleene algebras and rough sets. Electronic Notes in Theoretical Computer Science 225(5), 67–81 (2009).
- [19] Rao, A. S. and Georgeff, M.P. (1991). Modeling rational agents within a BID-architecture. In: R. Fikes and E. Sandewall (eds.), Proceedings of the Second Conference on Knowledge Representation and Reasoning, Morgan Kaufman.
- [20] Sebastian Thrun - Artificial Intelligence, 1998 – Elsevier, Learning metric-topological maps for indoor mobile robot navigation Pittsburgh, PA 15213, USA Received June 1996; revised October 1997.
- [21] R A Brooks, M J Mataric 1993- Robot learning, 1993 – Springer
- [22] Dunin-Keplicz, B. and Treur, J. (1995). Compositional formal specification of multi-agent systems. In: M. Wooldridge and N.R. Jennings, Intelligent Agents, Lecture Notes in Artificial Intelligence, Vol. 890, Springer Verlag, Berlin, pp. 102-117.
- [23] Nilsson, N. J. 1969, "Searching, problem solving, and game-playing trees for minimal cost solutions." In A.J. Morell (Ed.) IFIP 1968 Vol. 2, Amsterdam, North-Holland, 1556-1562, 1969.
- [24] M. Schmidt-Schauß, G. Smolka, Attributive concept descriptions with complements, Artificial Intelligence 48.
- [25] Giancarlo Guizzardi , 2005, Ontological Foundations for Structural Conceptual Models. CTIT, UTwenty, The Netherlands, PhD Thesis Series, No. 05-74 Telematica Instituut No. 015 (TI/FRS/015).

Rough Sets for Trees of Executions

Krzysztof Pancerz

Department of Computer Science, Faculty of Mathematics and Natural Sciences

University of Rzeszów, Poland

Email: kpancerz@ur.edu.pl

Abstract—In the paper, we propose to use rough sets to express some properties (reachability of states) of systems whose underlying models of behaviour are trees of executions. By analogy with the modal operators of branching time temporal logics, we define positive regions, boundary regions, and negative regions of anticipations of distinguished states (states of interest) in the modelled systems. Instead of a temporal logic approach, we propose to use a set theoretic approach.

I. INTRODUCTION

ROUGH sets [1] are an appropriate tool to deal with doubtful concepts in the universe U of discourse. A general idea of rough sets is to approximate a given set X of objects (states) of interest by other sets of objects (states), which are called the upper approximation $Upp(X)$ and the lower approximation $Low(X)$ of X , where $Low(X) \subseteq X \subseteq Upp(X)$. Approximation can be either exact (if $Low(X) = Upp(X)$) or rough (if $Low(X) \subset Upp(X)$). In terms of modal logics, the lower approximation can be identified with the necessity property, whereas the upper approximation can be identified with the possibility property (cf. [2]). Based on approximations, $Low(X)$ and $Upp(X)$, of the set X , the whole universe U of objects can be divided into three disjoint regions, the positive region $Pos(X)$, the negative region $Neg(X)$, and the boundary region $Bnd(X)$, where $Pos(X) = Low(X)$, $Neg(X) = U - Upp(X)$, and $Bnd(X) = Upp(X) - Low(X)$.

In [3] and [4], we proposed to use rough sets to describe some ambiguities in anticipation of states in systems whose dynamics is modelled by transition or timed transition systems. Analogously to rough approximation of sets, considered in rough set theory, we defined rough anticipation of states over transition (timed transition) systems. Anticipation of states was made via direct predecessor states of the anticipated ones. Therefore, this anticipation was called predecessor anticipation. We distinguished two kinds of anticipations, called the lower predecessor anticipation and the upper predecessor anticipation. Let X be a distinguished set of states we are interested to reach in a system whose behaviour is described by a transition system TS . The lower predecessor anticipation $LowPredAnt(X)$ consists of all states from which TS surely goes to the states in X as results of any events occurring at these states. It is necessary that each next state of any state from $LowPredAnt(X)$ is one of the states belonging to X . The upper predecessor anticipation consists of all states from which TS possibly goes to the states in X as results of some events occurring at these states. At least one next state of any state from $UppPredAnt(X)$ is the state belonging to X .

In this paper, we deal with a problem of identifying positive, negative and boundary regions of states of systems whose underlying models of behaviour are trees of executions. The proposed approach is patterned upon the temporal logic of branching time [5]. In this logic, the underlying model is mainly a tree of all possible computations. However, the presented approach is general and it can be applied to any system with the underlying tree model of behaviour. Instead of a temporal logic approach, we propose to use a set theoretic approach. We do not need to consider descriptions of system behaviours in terms of logical formulas. Therefore, we can build a tree of all possible paths of computations, paths of executions, paths of propagations, etc. Further, for simplicity, we will use a notion of a tree of executions. However, as it was mentioned earlier, any kind of dynamic actions can be considered (e.g. computations, executions, propagations, etc.). It is not necessary to identify nodes of trees with some propositions which can hold at these nodes. We can distinguish any states that should be reached, events that should happen, etc. Further, for simplicity, we will use a notion of a state. However, as it was mentioned earlier, any kind of entities can be considered (states, events, etc.).

In our approach, three kinds of anticipations of states, belonging to branches of a tree T of executions, are considered (see Section III). Let x be a state anticipating another states in a branch, we can distinguish:

- G-anticipation if $x \in T$ begins a branch consisting of states that are only the distinguished ones.
- F-anticipation if $x \in T$ begins a branch consisting of at least one state that is the distinguished one.
- X-anticipation if $x \in T$ begins a branch such that the next state in the branch is the distinguished one.

Because, a given state x can begin more than one branch, according to rough set theory, each kind of anticipation can be considered as either certain, possible, or impossible.

II. TEMPORAL LOGIC BACKGROUND

There is a variety of formal models of time. In instant-based models of time, the primitive temporal entities are time instants [6]. The flow of time is represented as a set of time instants with a binary relation of precedence on it. Two main types of instant-based models are usually considered:

- 1) Models with linear orderings of time instants, reflecting the idea that the time flow is a succession of time instants.

- 2) Models with partial orderings of time instants, reflecting the idea that the past is determined, while the future can be undetermined, branching into many possible time lines (there exist alternative futures).

With each time instant, a state (event, etc.) can be identified.

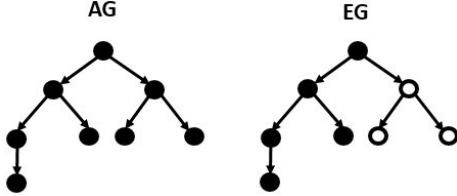


Fig. 1. AG and EG operators of branching time temporal logics

The term of temporal logic is broadly used to cover all approaches to representation and reasoning about time and temporal information within a logical framework [6]. In case of models with linear orderings of time instants, temporal logics are referred to as linear time temporal logics. Formulas of linear time temporal logics are interpreted over sequences of nodes corresponding to time instants. In case of models with partial orderings of time instants, temporal logics are referred to as branching time temporal logics. Formulas of branching time temporal logics are interpreted over trees of nodes corresponding to time instants.

Let T be a tree and s be a node in T . Let a be a proposition which can hold at some nodes in T . The following main modal operators are used in branching time temporal logics (cf. [5]):

- AGa holds at s if and only if a is true at all nodes of the subtree rooted at s (including s).
- EGa holds at s if and only if there is a path starting with s such that a is true at all nodes on this path.
- AFa holds at s if and only if on every path starting with s , there is some node at which a is true.
- EFa holds at s if and only if there is a path starting with s such that a is true at some node on this path.
- AXa holds at s if and only if a is true at every immediate successor of s .
- EXa holds at s if and only if a is true at some of immediate successor of s .

The meaning of the main operators of branching time temporal logics can be graphically explained as it is shown in Figures 1, 2, and 3. Filled circles represent nodes at which the proposition a is true. One can see that the first symbol (A or E) denotes quantification over branches, whereas the second symbol (G , F , or X) denotes quantification over states in the branches.

Temporal logics are used in various areas ranging from computer science (e.g. specification and verification of concurrent programs and systems), artificial intelligence (e.g. temporal representation and reasoning), and linguistics, to natural, cognitive and social sciences. In case of branching time temporal logics, the underlying model is a tree of all possible paths of computations, paths of executions, paths of propagations, etc.

III. DEFINITIONS AND EXAMPLE

In this section, the main idea of our approach is presented. Theoretical description is supplemented with a simple example illustrating the proposed approach.

A tree \mathbf{T} is a partially ordered set (poset) $\mathbf{T} = (T, R_<)$ such that for each $x \in T$ the set $\{y : (y, x) \in R_<\}$ is well-ordered by the binary relation $R_<$.

For a given tree $\mathbf{T} = (T, R_<)$, we can consider its subtree \mathbf{T}^x rooted at $x \in T$, i.e., $\mathbf{T}^x = (T^x, R_<)$ such that $T^x = \{y \in T : (x, y) \in R_< \text{ or } y = x\}$.

Let $\mathbf{T} = (T, R_<)$ be a tree. A segment $]a, b[$, where $a, b \in T$, is a set $]a, b[= \{x \in T : (a, x) \in R_< \text{ and } (x, b) \in R_<\}$. An element b is called a successor to an element a . An element a is called a predecessor to an element b . If $]a, b[= \emptyset$, then an element b is called an immediate successor to an element a and an element a is called an immediate predecessor to an element b .

Let $\mathbf{T} = (T, R_<)$ be a tree and $x \in T$. The set of all immediate successors of x is denoted by $Succ(x)$. The set of all immediate predecessors of x is denoted by $Pred(x)$. A leaf of \mathbf{T} is any element $x \in T$ such that $Succ(x) = \emptyset$. A chain of \mathbf{T} is any linearly ordered subset of T . A branch of \mathbf{T} is any maximal (with respect to a number of elements) chain of \mathbf{T} . A set of all leaves of \mathbf{T} is denoted by $Leaves(\mathbf{T})$. A set of all chains of \mathbf{T} is denoted by $Chains(\mathbf{T})$. A set of all branches of \mathbf{T} is denoted by $Branches(\mathbf{T})$.

Further, to refer to trees of executions, each element of a tree will be called a state.

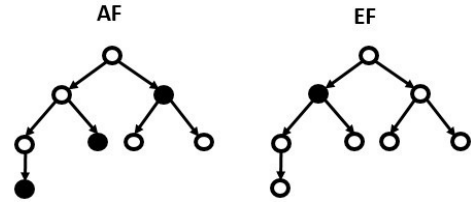


Fig. 2. AF and EF operators of branching time temporal logics

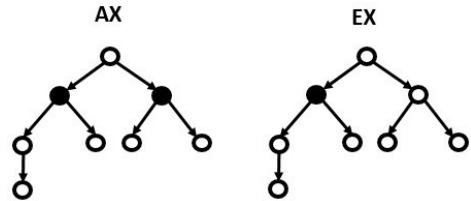


Fig. 3. AX and EX operators of branching time temporal logics

Let $\mathbf{T} = (T, R_<)$ be a tree and $S \subseteq T$ be a set of distinguished states in the tree \mathbf{T} . We can identify, in the set of states in the tree \mathbf{T} , the following regions:

- $PosAnt^G(S)$ - a positive region of G-anticipation of states from S .
- $BndAnt^G(S)$ - a boundary region of G-anticipation of states from S .

- $NegAnt^G(S)$ - a negative region of G-anticipation of states from S .
- $PosAnt^F(S)$ - a positive region of F-anticipation of states from S .
- $BndAnt^F(S)$ - a boundary region of F-anticipation of states from S .
- $NegAnt^F(S)$ - a negative region of F-anticipation of states from S .
- $PosAnt^X(S)$ - a positive region of X-anticipation of states from S .
- $BndAnt^X(S)$ - a boundary region of X-anticipation of states from S .
- $NegAnt^X(S)$ - a negative region of X-anticipation of states from S .

The division of regions given above corresponds to quantification over branches in the temporal logic of branching time.

Formal definitions of regions mentioned above are as follows. Let $\mathbf{T} = (T, R_<)$ be a tree and $S \subseteq T$. For each $x \in T$:

- $x \in PosAnt^G(S)$ if and only if

$$\forall_{B \in Branches(\mathbf{T}^x)} \forall_{y \in B} y \in S,$$

i.e., all branches started with x consist of only states belonging to S .

- $x \in BndAnt^G(S)$ if and only if

$$x \notin PosAnt^G(S) \text{ and } \exists_{B \in Branches(\mathbf{T}^x)} \forall_{y \in B} y \in S,$$

i.e., there is at least one branch started with x consisting of only states belonging to S , however not all branches started with x satisfy this condition.

- $x \in NegAnt^G(S)$ if and only if

$$x \notin PosAnt^G(S) \text{ and } x \notin BndAnt^G(S),$$

i.e., there is no branch started with x consisting of only states belonging to S .

- $x \in PosAnt^F(S)$ if and only if

$$\forall_{B \in Branches(\mathbf{T}^x)} \exists_{y \in B} y \in S,$$

i.e., all branches started with x consist of at least one state belonging to S .

- $x \in BndAnt^F(S)$ if and only if

$$x \notin PosAnt^F(S) \text{ and } \exists_{B \in Branches(\mathbf{T}^x)} \exists_{y \in B} y \in S,$$

i.e., there is at least one branch started with x consisting of at least one state belonging to S , however not all branches started with x satisfy this condition.

- $x \in NegAnt^F(S)$ if and only if

$$x \notin PosAnt^F(S) \text{ and } x \notin BndAnt^F(S),$$

i.e., there is no branch started with x consisting of at least one state belonging to S .

- $x \in PosAnt^X(S)$ if and only if

$$\forall_{y \in Succ(x)} y \in S,$$

i.e., all branches started with x are such that an immediate successor of x belongs to S .

- $x \in BndAnt^X(S)$ if and only if

$$x \notin PosAnt^X(S) \text{ and } \exists_{y \in Succ(x)} y \in S,$$

i.e., there is at least one branch started with x such that an immediate successor of x belongs to S , however not all branches started with x satisfy this condition.

- $x \in NegAnt^X(S)$ if and only if

$$x \notin PosAnt^X(S) \text{ and } x \notin BndAnt^X(S),$$

i.e., there is no branch started with x such that an immediate successor of x belongs to S .

One can see that:

- if $x \in Leaves(\mathbf{T})$ and $x \in S$, then $x \in PosAnt^G(S)$ and $x \in PosAnt^F(S)$,
- if $x \in Leaves(\mathbf{T})$ and $x \notin S$, then $x \in NegAnt^G(S)$ and $x \in NegAnt^F(S)$,
- if $x \in Leaves(\mathbf{T})$, then $x \in NegAnt^X(S)$,
- if $x \notin Leaves(\mathbf{T})$ and $x \in PosAnt^G(S)$, then $x \in PosAnt^F(S)$ and $x \in PosAnt^X(S)$.

Let us consider a tree \mathbf{T} shown in Figure 4. For the set

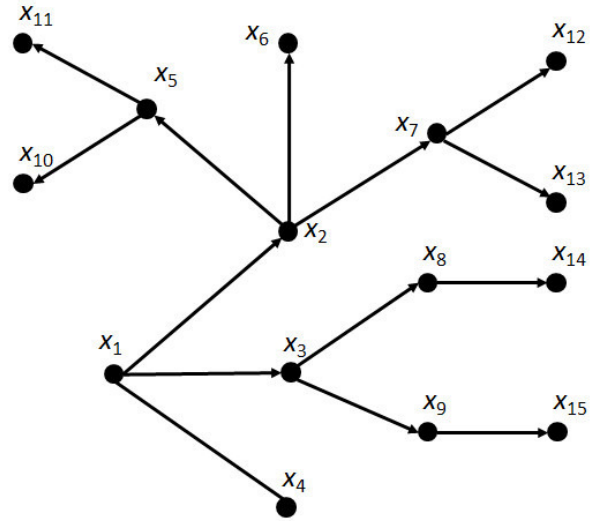


Fig. 4. A tree \mathbf{T} modeling some executions.

$$S = \{x_3, x_7, x_8, x_{12}, x_{13}, x_{14}\}$$

of distinguished states of the tree \mathbf{T} , we obtain:

- $x_1 \in NegAnt^G(S)$ and $x_1 \in BndAnt^F(S)$ and $x_1 \in BndAnt^X(S)$,
- $x_2 \in NegAnt^G(S)$ and $x_2 \in BndAnt^F(S)$ and $x_2 \in BndAnt^X(S)$,
- $x_3 \in BndAnt^G(S)$ and $x_3 \in PosAnt^F(S)$ and $x_3 \in BndAnt^X(S)$,
- $x_4 \in NegAnt^G(S)$ and $x_4 \in NegAnt^F(S)$ and $x_4 \in NegAnt^X(S)$,

- $x_5 \in NegAnt^G(S)$ and $x_5 \in NegAnt^F(S)$ and $x_5 \in NegAnt^X(S)$,
- $x_6 \in NegAnt^G(S)$ and $x_6 \in NegAnt^F(S)$ and $x_6 \in NegAnt^X(S)$,
- $x_7 \in PosAnt^G(S)$ and $x_7 \in PosAnt^F(S)$ and $x_7 \in PosAnt^X(S)$,
- $x_8 \in PosAnt^G(S)$ and $x_8 \in PosAnt^F(S)$ and $x_8 \in PosAnt^X(S)$,
- $x_9 \in NegAnt^G(S)$ and $x_9 \in NegAnt^F(S)$ and $x_9 \in NegAnt^X(S)$,
- $x_{10} \in NegAnt^G(S)$ and $x_{10} \in NegAnt^F(S)$ and $x_{10} \in NegAnt^X(S)$,
- $x_{11} \in NegAnt^G(S)$ and $x_{11} \in NegAnt^F(S)$ and $x_{11} \in NegAnt^X(S)$,
- $x_{12} \in PosAnt^G(S)$ and $x_{12} \in PosAnt^F(S)$ and $x_{12} \in NegAnt^X(S)$,
- $x_{13} \in PosAnt^G(S)$ and $x_{13} \in PosAnt^F(S)$ and $x_{13} \in NegAnt^X(S)$,
- $x_{14} \in PosAnt^G(S)$ and $x_{14} \in PosAnt^F(S)$ and $x_{14} \in NegAnt^X(S)$,
- $x_{15} \in NegAnt^G(S)$ and $x_{15} \in NegAnt^F(S)$ and $x_{15} \in NegAnt^X(S)$.

We leave the reader with the proof of the assignments above.

IV. CONCLUSIONS

We have shown that rough sets can be used to express some properties (reachability of states) of systems whose underlying models of behaviour are trees of executions. The proposed

approach is patterned upon the temporal logic of branching time, however a set theoretic approach causes that we do not need to consider system behaviours in terms of logical formulas. A challenging problem for further investigation is to consider anticipations of states in terms of the Variable Precision Rough Set Model [7] as well as fuzzy rough sets and rough fuzzy sets [8].

REFERENCES

- [1] Z. Pawlak, *Rough Sets. Theoretical Aspects of Reasoning about Data*. Dordrecht: Kluwer Academic Publishers, 1991.
- [2] Y. Yao and T. Lin, "Generalization of rough sets using modal logics," *Intelligent Automation and Soft Computing*, vol. 2, no. 2, pp. 103–120, 1996. doi: 10.1080/10798587.1996.10750660
- [3] K. Pancerz and A. Schumann, "Rough set models of Physarum machines," *International Journal of General Systems*, vol. 44, no. 3, pp. 314–325, 2015. doi: 10.1080/03081079.2014.997529
- [4] A. Schumann and K. Pancerz, "Roughness in timed transition systems modeling propagation of plasmodium," in *Rough Sets and Knowledge Technology*, ser. Lecture Notes in Artificial Intelligence, D. Ciucci, G. Wang, S. Mitra, and W.-Z. Wu, Eds. Springer International Publishing, 2015, vol. 9436, pp. 482–491.
- [5] M. Ben-Ari, A. Pnueli, and Z. Manna, "The temporal logic of branching time," *Acta Informatica*, vol. 20, no. 3, pp. 207–226, 1983. doi: 10.1007/BF01257083
- [6] V. Goranko and A. Galton, "Temporal logic," in *The Stanford Encyclopedia of Philosophy*, winter 2015 ed., E. N. Zalta, Ed. Metaphysics Research Lab, Stanford University, 2015.
- [7] W. Ziarko, "Variable precision rough set model," *Journal of Computer and System Sciences*, vol. 46, no. 1, pp. 39–59, 1993. doi: 10.1016/0022-0000(93)90048-2
- [8] D. Dubois and H. Prade, "Rough fuzzy sets and fuzzy rough sets," *International Journal of General Systems*, vol. 17, no. 2-3, pp. 191–209, 1990. doi: 10.1080/03081079008935107

Evaluation of classifiers: current methods and future research directions

Katarzyna Stapor

Silesian University of Technology
 ul. Akademicka 16, 44-100 Gliwice, Poland
 Email: Katarzyna.Stapor@polsl.pl

Abstract—This paper aims to review the most important aspects of the classifier evaluation process including the choice of evaluating metrics (scores) as well as the statistical comparison of classifiers. Some recommendations, limitations of the described methods as well as the future, promising directions are presented. This article provides a quick guide to understand the complexity of the classifier evaluation process and tries to warn the reader about the wrong habits.

I. PROBLEM DESCRIPTION

LEARNING A CLASSIFIER from a dataset of labeled data instances taken from unknown distribution where each instance is characterized by a feature vector and a class to which it belongs is a central task of supervised classification. A learned classifier is a function mapping whole feature space into a label space. Then, the learned classifier, after evaluation its quality, can be used to classify new samples with unknown class label. There are many classification paradigms/models: the detailed description of the supervised classification problem can be found in books on machine learning (see for example [1]). The following question usually arises: “which is the best classification paradigm for a given problem?”. Answering this question requires the evaluation as well as the comparison of the many candidate models. Usually, the problem of classifier evaluation is performed by using the scores that try to summarize the specific conditions of classifier behavior. The examples of such scores are classification error or accuracy. It is now generally agreed that the whole evaluation process of a classifier should include the following steps ([4], [5], [6], [10], [11], [12]):

- 1) choosing the score(s) according to the properties of the classifier as well as the domain objectives,
- 2) choosing the score estimation method,
- 3) choosing the statistical test,
- 4) choosing the datasets,
- 5) running the evaluation.

The main purpose of this paper is to provide the reader with a better understanding about the overall classifier evaluation process. As there is no fixed, concrete recipe for the classifier evaluation procedure, we believe that this paper will facilitate the researcher in the machine learning area to decide which alternative to choose for each specific case.

This paper is focused only on a supervised classification problem as defined in the beginning. Other types of classification such as classification from data streams or multi-label

TABLE I
 CONFUSION MATRIX FOR A TWO-CLASS PROBLEM

	Predicted positive	Predicted negative
Positive class	True Positive (TP)	False Negative (FN)
Negative class	False Positive (FP)	True Negative (TN)

classification are not addressed here, since they may impose specific conditions to the calculation of the score.

The paper is set up as follows. In section 2 till 4 we shortly present the mentioned steps of classifier evaluation. In section 5 we conclude giving some recommendations and propose new, future directions for classifier evaluation methodology.

II. CHOOSING CLASSIFIER SCORES

Typical scores for measuring the performance of a classifier are accuracy and classification error, which for a two-class problem can be easily derived from a 2x2 confusion matrix as that given in table reftable1. These scores can be computed as:

$$Acc = (TP + TN)/(TP + FN + TN + FP)$$

$$Err = (FP + FN)/(TP + FN + TN + FP)$$

Empirical evidence shows that accuracy and error rate are biased with respect to data imbalance: the use of these scores might produce misleading conclusions since they are strongly biased to favor the majority class, and are sensitive to class skews.

In some application domains, we may be interested in how our classifier classifies only a part of the data, i.e. positive or negative data samples. Examples of such measures are: True positive rate (Recall or Sensitivity): $TPrate = TP/(TP + FN)$, True negative rate (Specificity): $TNrate = TN/(TN + FP)$, Precision = $TP/(TP + FP)$.

Each entry in the confusion matrix may be misleading by two confounding issues: asymmetric misclassification costs and asymmetric class distributions. Shortcomings of the accuracy or error rate have motivated search for new balanced measures which aim to obtain a trade-off between the evaluation of the classification ability on both positive and negative data samples. Some straightforward examples of such alternative scores are: the arithmetic, geometric or harmonic means between Recall and Specificity. They give the same relevance to both components. There are other proposals that

try to enhance one of the two components of the mean. For instance, Index of Balanced Accuracy [7]:

$$IBA_\alpha = (1 + \alpha(TPrate - TNrate)) \times TPrate \times TNrate$$

and F -score [14]:

$$F\text{-score}_\beta = \frac{(\beta^2 + 1)Precision \times Recall}{\beta^2 \times Precision + Recall}$$

The parameters α, β can be tuned to obtain different trade-offs between both components.

The cost matrix can be used if the severity of misclassifications can be quantified in terms of costs and then, to weight the entries in the confusion matrix. When the classification costs cannot be accessed, the above mentioned balanced scores may be used to set more relevance to the costliest misclassification. Another most widely-used technique in this case is the ROC curve [3]. However, recent studies have shown that AUC (Area under the ROC curve) is a fundamentally incoherent measure since it treats the costs of misclassification differently for each classifier. This is undesirable because the cost must be a property of the problem, not of the classification method. In [8], the H measure has been proposed as an alternative to AUC.

Ground truth assumption states that the true class labels of data samples are deterministically known even though they are the result of an arbitrary unknown distribution that a classifier aims to approximate. This make it impossible to take into account that correct classification could be a result of coincidental concordance between classifier's output and label-generation process. Cohen's kappa statistics corrects for this problem:

$$\kappa = \frac{P_o - P_o^c}{1 - P_o^c}$$

where P_o represents the probability of overall agreement over the label assignments between the classifier and the true process, and P_o^c represents the chance agreement over the labels as is defined as the sum of the proportion of examples assigned to a class times the proportion of true labels of that class in the dataset.

Performance measures for multi-class classification are still an open research topic. Generally, the two approaches are commonly used. Macroaveraging (per category) takes the average of measures on separate classes:

$$B_{macro} = \frac{1}{n} \sum_{i=1}^n B(TP_i, FP_i, FN_i, TN_i)$$

where B is a binary score. Microaveraging (per case) sums up individual TP, FP, FN, TN for different classes and then apply to get a measure:

$$B_{micro} = B\left(\sum_{i=1}^n TP_i, \sum_{i=1}^n FP_i, \sum_{i=1}^n FN_i, \sum_{i=1}^n TN_i\right)$$

There is no complete agreement among the authors on which is better. In this paper, we focus on the scores since they are popular way to measure classification quality. But these

measures do not capture all the information about the quality of classification methods some graphical methods may do. The presented list of scores is by no means exhaustive. There are other important aspects of classification such as robustness to noise, scalability, stability under data shifts, etc. which are not addressed here.

III. CHOOSING SCORE ESTIMATION METHOD

Various re-sampling methods are commonly used to estimate the classifier scores (the review of re-sampling methods can also be found in the mentioned literature on machine learning). The most commonly used k -fold cross-validation (CV) creates a k -fold partition of the entire dataset once. Then, for each of k experiments, it uses $(k-1)$ folds for training and a different fold for testing. The classification error is estimated as the average of separate errors obtained from k experiments. In order to obtain more stable estimates, it is useful to perform multiple runs of simple re-sampling schemes. Two specific schemes has been suggested: 5x2CV and 10x10CV.

The danger of re-sampling is that it is usually followed by statistical testing which relies on the fundamental assumption that the data used to obtain the sample must be independent. In re-using the data, this important assumption is broken and the results of the statistical test are invalid.

IV. CHOOSING STATISTICAL TEST

In most situations, the statistical assessment of the observed classifier scores such as hypothesis testing is required. For the comparison of two classifiers on one dataset, the corrected resampled t test has been suggested in the literature [2]. This test is associated with a repeated estimation method: in i -th of the m iterations, a random data partition is conducted and the values for the scores $A_{k1}^{(i)}$ and $A_{k2}^{(i)}$ of compared classifiers $k1$ and $k2$, are obtained. The statistic is:

$$t = \frac{\bar{A}}{\sqrt{\left(\frac{1}{m} + \frac{N_{test}}{N_{train}}\right) \cdot \sum_{i=1}^m \frac{(A^{(i)} - \bar{A})^2}{m-1}}}$$

where $\bar{A} = \frac{1}{m} \sum_{i=1}^m A^{(i)}$, $A^{(i)} = \left(A_{k1}^{(i)} - A_{k2}^{(i)}\right)$, N_{test} , N_{train} are the number of samples in the test and train partitions. A non-parametric alternative for comparing two classifiers that is suggested in the literature is McNemar's test [9].

For the comparison of two classifiers on multiple datasets the Wilcoxon signed-ranks test [9] is widely recommended. It ranks the differences $d_i = A_{k1}^{(i)} - A_{k2}^{(i)}$ between scores of two classifiers $k1$ and $k2$ obtained on i -th of N datasets, ignoring the signs. The test statistic of this test is:

$$T = \min(R^+, R^-)$$

where:

$$R^+ = \sum_{d_i > 0} \text{rank}(d_i) + \frac{1}{2} \sum_{d_i = 0} \text{rank}(d_i),$$

$$R^- = \sum_{d_i < 0} \text{rank}(d_i) + \frac{1}{2} \sum_{d_i = 0} \text{rank}(d_i)$$

are the sums of ranks on which the k_2 classifier outperforms k_1 , respectively. Ranks $d_i = 0$ are split evenly among the sums.

Comparison among multiple classifiers on multiple datasets, the general recommended methodology is as follows. First, we apply an omnibus test to detect if at least one of the classifiers performs different than the others. Friedman nonparametric test [9] with Iman-Davenport extension is probably the most popular omnibus test. It is a good choice when comparing more than five different classifiers. Let R_{ij} be the rank of the j -th of K classifiers on the i -th of N data sets and

$$R_j = \frac{1}{N} \sum_{i=1}^N R_{ij}$$

is the mean rank of the j -th classifier. The test compares the mean ranks of the classifiers and is based on the test statistic:

$$F_F = \frac{(N-1)\chi_F^2}{N(K-1) - \chi_F^2}$$

$$\chi_F^2 = \frac{12N}{K(K+1)} \left[\sum_{j=1}^K R_j^2 - \frac{K(K+1)^2}{4} \right]$$

which follows an F distribution with $(K-1)$ and $(K-1)(N-1)$ degrees of freedom.

For the comparison of five or less different classifiers, Friedman aligned ranks [9] is a more powerful alternative.

Second, if we find such a significant difference, then we apply a pairwise test with the corresponding post-hoc correction for multiple comparisons to control the family-wise error [13]. For the described above Friedman test, comparing the r -th and s -th classifiers is based on the mean ranks and has the form:

$$z = \frac{R_r - R_s}{\sqrt{\frac{K(K+1)}{6N}}}$$

The z value is used to find the corresponding probability from the table of normal distribution, which is then compared with an appropriate significance level α . There are multiple proposals in the literature to adjust the significance level α : for example, Holm, Hochberg, Finner [9].

V. DATASET SELECTION

The commonly accepted approach in classifier evaluation methodology is to use benchmark datasets as a representation of all the classification problems that can arise in reality and then, to demonstrate that one classifier is, on average, better than the others. However, such representation assumption is questionable as well as the following conclusions (i.e. the generalization to unseen problems).

No free lunch theorem [15] states that for any two classifiers, there are as many classification problems for which the first classifier performs better than the second as vice versa. Thus, it does not make sense to demonstrate that one classifier is, on average, better than the others. Instead, we should focus our attention on exploring the conditions of the classification

problems which make our classifier to perform better or worse than others. Additionally, artificially generated datasets may easily reproduce the specific conditions of interest.

VI. RECOMMENDATIONS AND FUTURE DIRECTIONS

The evaluation of classification performance is very important to the construction and selection of classifiers. Below, we give some recommendations and limitations of the presented methods for classifier evaluation. We also try to define new promising research directions.

- There are many scores for evaluating classifiers: generally, you shouldn't take any of the existing scores in an isolated way. No single metric is capable of encapsulated all the aspects of interest. Multiple metrics need to be reported to detail classifier's performance even for a single aspect of interest. There is not a best way to evaluate any system, but different scores give us different and valuable insights into how a classification model performs. *Many research efforts should be undertaken to investigate principles of combining these scores to yield a summary measure.*
- The vast majority of the published articles use the accuracy (or classification error) as the score in the classifier evaluation process. But these two scores may be appropriate only when the datasets are balanced and the misclassification costs are the same for false positives and false negatives. In the case of skew datasets, which is rather typical situation, the accuracy/error rate is questionable and other scores, especially balanced scores such as Index of Balanced Accuracy, F-score, geometric or harmonic means, H measure are more appropriate. *New methods that aim to obtain a trade-off between the evaluation of the classification ability on both positive and negative classes are need to be developed.*
- Ground truth assumption make it impossible to take into account that correct classification could be a result of coincidental concordance between classifier's output and label-generation process. Cohen's kappa is the simplest measure that corrects for this problem. *New, better chance-corrected measures of the validity of classifiers are needed.*
- In the case of multi-class classification, generally, macroaveraging can be bad practice in cases that there is a considerable difference in number of examples of each class label. Actually, the majority believe that class examples should indeed count proportionally to their frequency, and thus lean towards microaveraging. But, there is no complete agreement among authors on which is better. *Performance measures for multi-class classification are still an open research topic and many empirical investigations are needed.*
- k -fold cross-validation is the best known resampling technique which is commonly used in score estimation. Through high overlapping in the training folds, main independence assumption of many statistical tests used further for statistical comparison is not fulfilled. *This can*

affect the bias of the classifier score and requires new, corrected versions of classical statistical tests which still should be developed.

- In order to obtain more stable estimates of classifier performance, it is useful to perform multiple runs of simple re-sampling schemes. Two such schemes are recommended: 5x2CV and 10x10CV. *More experiments on different schemes are needed to investigate replicability of the results.*
- The comparison of two classifiers on a single dataset is generally unsafe due to the lack of independence between the obtained score values. *Thus, the new corrected versions of the resampled t test or t test for repeated cross-validation are more appropriate.* McNemar's test, being non-parametric, does not make the assumption about distribution of the scores but it does not directly measure the variability due to the choice of the training set nor the internal randomness of the learning algorithm.
- When comparing two classifiers on multiple datasets (especially from different sources), the measured scores are hardly commensurable. Therefore, the *Wilcoxon signed-rank test* is more appropriate.
- Regarding the comparison of multiple classifiers on multiple datasets, if the number of classifiers involved is higher than five, the use of the Friedman test with Iman and Davenport extension is recommended. When this number is low, four or five, Friedman aligned ranks and the Quade test are more useful. If the null hypothesis has been rejected, we should proceed with a post-hoc test to check the statistical differences between pairs of classifiers. The multiple comparisons are usually performed using the mean-ranks test. *Because of fundamental inconsistencies of this test we discourage its use in machine learning. To overcome these issues, we suggest instead to perform the multiple comparison using a test whose outcome only depends on the two algorithms being compared, such as the sign-test or the Wilcoxon signed-rank test.*
- Regarding dataset selection, we must carefully choose the datasets to be included in the evaluation process to reflect the specific conditions, for example class imbalance, classification cost, dataset size, application domain, etc. *The choice of the datasets should be guided in order*

to identify specific conditions that make a classifier to perform better than others.

Summarizing, this review tries to provide the reader with a better understanding about the overall process of classifier evaluation. We believe, that this review can improve the way in which researchers and practitioners in machine learning contrast the results achieved in their experimental studies using statistical methods. The propositions mentioned above (in italic) can direct researchers in their work on the new, better solutions for classifier evaluation procedures.

REFERENCES

- [1] Bishop Ch. "Pattern recognition and machine learning," Springer, New York, 2006.
- [2] Bouckaert R., "Estimating replicability of classifier learning experiments," Proc. 21st Conf. ICML, AAAI Press, 2004, <http://dx.doi.org/10.1145/1015330.1015338>.
- [3] Bradley P., "The use of the area under the ROC curve in the evaluation of machine learning algorithms," Pattern recognition, 30, 1997, pp. 1145–1159, [http://dx.doi.org/10.1016/S0031-3203\(96\)00142-2](http://dx.doi.org/10.1016/S0031-3203(96)00142-2).
- [4] Dietterich T., "Approximate statistical tests for comparing supervised classification learning algorithms," Neural Computation, 10, 1998, pp. 1895–1924, <http://dx.doi.org/10.1162/089976698300017197>.
- [5] Demsar J., "Statistical comparison of classifiers over multiple data sets," Journal of Machine Learning Research, 7, 2006, pp. 1–30.
- [6] Garcia S. Fernandez A., Lutengo J. and Herrera F., "Advanced non-parametric tests for multiple comparisons in the design of experiments in the computational intelligence and data mining: experimental analysis of power," Inf. Sci., 180(10), 2010, pp. 2044–2064, <http://dx.doi.org/10.1016/j.ins.2009.12.010>.
- [7] Garcia V. et. al., "Index of balanced accuracy: a performance measure for skewed class distributions," 4th IbPRIA, 2009, pp. 441–448, http://dx.doi.org/10.1007/978-3-642-02172-5_57.
- [8] Hand D., "Measuring classifier performance: a coherent alternative to the area under the ROC curve," Machine Learning, 77, 2009, pp. 103–123, <http://dx.doi.org/10.1007/s10994-009-5119-5>.
- [9] Hollander M. and Wolfe D., "Nonparametric statistical methods," John Wiley & Sons, 2013, <http://dx.doi.org/10.1002/9781119196037>.
- [10] Japkowicz N. and Shah M., "Evaluating learning algorithms: a classification perspective," Cambridge University Press, Cambridge, 2011.
- [11] Salzberg S., "On comparing classifiers: pitfalls to avoid and recommended approach," Data Mining and Knowledge Discovery, 1, 1997, pp. 317–328, <http://dx.doi.org/10.1023/A:1009752403260>.
- [12] Santafe G. et. al., "Dealing with the evaluation of supervised classification algorithms," Artif. Intell. Rev. 44, 2015, pp. 467–508, <http://dx.doi.org/10.1007/s10462-015-9433-y>.
- [13] Shaffer J. P., "Multiple hypothesis testing," Annual Review of Psychology, 46, 1995, pp. 561–584.
- [14] Sokolova M. and Lapalme G., "A systematic analysis of performance measures for classification tasks," Inf. Proc. and Manag., 45, 2009, pp. 427–437, <http://dx.doi.org/10.1016/j.ipm.2009.03.002>.
- [15] Wolpert D., "The lack of a priori distinctions between learning algorithms," Neural Comput. 8(7), 1996, pp. 1341–1390, <http://dx.doi.org/10.1162/neco.1996.8.7.1341>.

7th International Workshop on Artificial Intelligence in Medical Applications

THE workshop on Artificial Intelligence in Medical Applications – AIMA'2017—provides an interdisciplinary forum for researchers and developers to present and discuss latest advances in research work as well as prototyped or fielded systems of applications of Artificial Intelligence in the wide and heterogenous field of medicine, health care and surgery. The workshop covers the whole range of theoretical and practical aspects, technologies and systems based on Artificial Intelligence in the medical domain and aims to bring together specialists for exchanging ideas and promote fruitful discussions.

TOPICS

- Artificial Intelligence Techniques in Health Sciences
- Knowledge Management of Medical Data
- Data Mining and Knowledge Discovery in Medicine
- Health Care Information Systems
- Clinical Information Systems
- Agent Oriented Techniques in Medicine
- Medical Image Processing and Techniques
- Medical Expert Systems
- Diagnoses and Therapy Support Systems
- Biomedical Applications
- Applications of AI in Health Care and Surgery Systems
- Machine Learning-based Medical Systems
- Medical Data- and Knowledge Bases
- Neural Networks in Medicine
- Ontology and Medical Information
- Social Aspects of AI in Medicine
- Medical Signal and Image Processing and Techniques
- Ambient Intelligence and Pervasive Computing in Medicine and Health Care

SECTION EDITORS

- **Lasek, Piotr**, University of Rzeszow, Poland
- **Paja, Wiesław**, University of Rzeszów, Poland
- **Pancerz, Krzysztof**, University of Rzeszów, Poland

REVIEWERS

- **Bamidis, Panagiotis**, o Aristotle University of Thessaloniki, Greece
- **Ciureanu, Adrian**, University of Medicine and Pharmacy from Iasi, Romania
- **Iantovics, Barna**, Petru Maior University, Romania
- **Jónsson, Björn Þór**, IT University of Copenhagen, Denmark
- **Komenda, Martin**, Institute of Biostatistics and Analyses, Faculty of Medicine, Masaryk University, Brno, Czech Republic
- **Komenda, Martin**, Masaryk University, Czech Republic
- **Kononowicz, Andrzej**, Jagiellonian University Medical College, Poland
- **Leniowska, Lucyna**, University of Rzeszow, Poland
- **Majernik, Jaroslav**, Pavol Jozef Safarik University in Kosice, Slovakia
- **Mapayi, Temitope**, University of KwaZulu-Natal, Durban, South Africa, South Africa
- **Olszewska, Joanna Isabelle**, University of Gloucestershire, United Kingdom
- **Papagelis, Manos**, York University, Canada
- **Perner, Petra**, IBAI Leipzig, Germany
- **Pokorná, Andrea**, Institute of Biostatistics and Analyses, Faculty of Medicine, Masaryk University, Brno
- **Rabl, Tilmann**, Technische Universität, Berlin, Germany
- **Schwarz, Daniel**, Masaryk University, IBA, Czech Republic
- **Stańczyk, Urszula**, Silesian University of Technology, Poland
- **Subbotin, Sergey**, Zaporizhzhya National Technical University, Ukraine
- **Víta, Martin**, Faculty of Informatics, Masaryk university, Czech Republic
- **Woodham, Luke**, St George's University of London
- **Yakovets, Nikolay**, Eindhoven University of Technology, The Netherlands
- **Zaitseva, Elena**, University of Zilina, Slovakia
- **Zary, Nabil**, Nanyang Technological University

A Deep Learning-Based Approach for the Recognition of Sleep Disorders in Patients with Cognitive Diseases: A Case Study

Giovanni Paragliola, Antonio Coronato

Abstract—Alzheimer’s disease is the most common type of dementia. Patients suffer from of this kind of disease could show symptoms such as sleep disturbances, muscle rigidity or other typical Alzheimer’s movement irregularities. In our work, we have focused on those types of disturbances related to sleep disorders. Due to their not well-known nature, it is difficult to develop software able to identify sleep disorders. In this work, we have addressed the problem of the automatic recognition of sleep disorders in patients with Alzheimer’s disease by using deep learning algorithms.

Index Terms—Deep Learning, Convolutional Neural Network, Deep Neural Network, Human Behaviors Recognition

I. INTRODUCTION

THE aging of the world population during the last few decades has been highlighting problems related to the increase in the incidence of cognitive diseases such as dementia and consequent issues about how to assist those patients who suffer from them.

Alzheimer’s disease (AD) is the most common type of dementia. Patients with AD could show symptoms such as sleep disturbance, well-formed visual hallucinations, muscle rigidity or other typical Alzheimer’s movement irregularities.

In this work, we have focused on those types of disturbances related to sleep disorders (SD).

The strong correlation between sleep disorders and Alzheimer disease has been highlighted in a lot of works in which showing that changes in sleep patterns may predict Alzheimer disease [1], [2].

The study of sleeping disorders, in particular, the ones related to movements such as agitation and restless sleep, take on an important role for an early prediction and prevention of AD and more in general of cognitive diseases.

The etiology of these kinds of disorders is unknown[3], for this reason, ICT technologies should provide solutions able to accurately recognize these kinds of disorders.

In order to recognize anomalous behaviors it is basic to monitor patients during their lifetime, we have been already facing the challenge of monitoring patients with cognitive diseases by proposing methodologies and approaches for the design of systems aimed to achieve this task [4], [5].

In this work, we have addressed the problem of the recognition of a sleep agitation disorders in patients with Alzheimer’s

disease.

The purpose of our study is to identify two sleep states: { *Normal Sleep* (N), *Anomalous Sleep* (A) }.

A normal sleep is a state in which a patient sleeps calm, an anomalous sleep is a state in which there are anomalous movements characterized by a strong agitation.

The main issues related to the recognition of such kinds of disorders is their unknown and unpredictable nature; in other words, there are not well-known patterns which describe how these disorders arise, for this reason, the development of system able to automatically recognize them it is quite hard.

We have faced the problem of identification of sleep disorders in [6] by means of threshold-based approach. The main limitation was the identification of the best values of the threshold to avoid a high false positive rate (FP) and guarantee a good level of accuracy of the identification of the disorders. This issue was due to the strong dependency between the threshold and the patient’s movements that made the approach complex to tune and patient-dependent.

In order to overcome the problem of high FP and develop a patient-independent solution, we have defined a deep learning based approach for both the classification of sleep disorders and identification of sleep states.

In order to provide an initial level of validation of our solution, we have monitored one pilot patient with Alzheimer’s disease and recorded both its movements and stress level.

We have created a preliminary dataset by monitoring an amount of seven nights.

The aim of our work is to classify the anomalous sleep states of the patient during the night by analyzing both the movements and EDA signals.

We have extracted two biometric signals: the movements and the stress level of the patient. Both signals have been acquired by means of a sensor placed on his right leg, the *E4 wristband* sensor [7].

The movements are described by means of the 3-axes acceleration values and the stress level is described by the electrodermal activity (EDA).

We have used these signals as input for two kinds of deep learning (DL) algorithms: deep neural network (DNN) [8] and conventional neural network (CNN) [8].

In this paper, we present the results of the application of those algorithms for the classification of the sleep states of the patient in order to automatically recognize the anomalous ones.

In our first experiment, the results have demonstrated that our

Giovanni Paragliola and Antonio Coronato in National Research Council (CNR) Institute for High-Performance Computing and Networking (ICAR) , Italy, Naples, ITA e-mail: ({giovanni.paragliola, antonio.coronato}@icar.cnr.it).



Fig. 1. Polysomnography ¹

solution is able to recognize and classify the patients' status both with DNN and CNN.

The results show a better performance of the CCN with an overall accuracy ranges from 80 % to 89% against the accuracy of DNN ranges from 50% to 80%.

II. RELATED WORK

Today the gold standard, for the treating of sleep disorders is the polysomnography, a type of sleep study, which involves the acquisition of data from a multi-parametric test used in the study of sleep and as a diagnostic tool in sleep medicine.

Although the polysomnography is the main treatment for sleep studies, it has a few drawbacks: (i) the procedure is quite disturbing due to the huge amount of wearing sensors (e.g. Fig 1) (ii) it must be performed in hospital environment only (iii) it has been performed when the subject is already aware that he/she may be suffer from the disease.

Our solution has been designed to overcome the first two points.

Our approach uses only one multi-parameters sensor which can be used at home without clinical support.

Other out-of-hospital solutions focus their effort on the study of Electroencephalography (EEG) in order to detect anomalies during the sleep with results obtained through the use of uncomfortable devices.

Poree et al [9] proposed a sleep recording system to perform the monitoring of sleeping disorders; the solution adopts five electrodes: two temporal, two frontal and one reference.

In [10] authors proposed a video-polysomnography method to determine sleep disorders. At first, they used an infrared night-vision video webcam for recording a polysomnographic video during sleep period at night and using a motion detection algorithm over the captured images.

Although the approaches widely used are based on EEG/EMG signals, other kinds of parameters have been adopted. An example is provided by Flores et al [11]. In their work, the authors used a motion sensor to catch significant body movements. During waking time, respiratory movements are masked by other motor activities. An automatic pattern recognition system has been developed to identify periods of sleep and waking using a piezoelectric generated signal.

Prashanth et al [12] adopted an olfactory loss and REM

features to develop support vector machine-based prediction models using data from the Parkinson's Progression Marker's Initiative (PPMI) database.

Alves de Mesquita et al [13] present a monitoring system to recognize sleep breathing disorders by means of nasal pressure recording technique.

Occhiuzzi et al [14] investigate the feasibility of using a passive RF identification technology for the wireless monitoring of human body movements in some common sleep disorders by means of passive tags equipped with inertial switches.

Park et al [15] proposed an accelerometer-based solution for the classification of the state of healthy users to "sleep" or "wakefulness". The authors face the problem of misclassification rate by employing a dynamic classifier which analyzes similarity between the neighboring data scores obtained from support vector machine classifier.

III. APPROACH

In this section we describe the approach that we have adopted for the classification of the sleep stages. We have set two kinds of experiments: one by using CNN and another one by using DNN.

The aim of this work is to evaluate how well deep learning algorithms, such as CNN and DNN, work for the classification of sleep states by taking in input biomedical signals like movements and EDA.

In Figure 2 we have highlighted (green line) an example of anomaly period that we have identified in our previous work [6].

We define *anomaly* that period because by comparing how the patient has moved in with the other periods, it is clear that its movements were strangely stronger.

In [6] we detected such as periods by a thresholds-based approach that evaluated the *intensity* of the patient's movement. The anomalous behaviors of the movements signal are clear and well-characterized, unlike the EDA.

The input of our process is a couple of biomedical signals: the movements of the patients and the stress level.

The first one is described by means of XYZ acceleration measure, the second one by means of electrodermal activity (EDA). Both signals have acquired by the same sensor, *E4 wristband*.

The E4 Wristband is a Bluetooth sensor for the acquisition of biomedical data of patients such as body temperature and stress level and movements.

For the purpose of this paper, we focus only on acceleration signals (x,y,z) and the stress level (EDA). The data have been acquired with a sample rate of 32 Hz(f0). The dynamic of the amplitude of the acceleration was [-2G,2G].

The first step was to collect the data, in order to do that we have placed the E4 sensor on the patient's leg who has been monitored for one week each night for an amount of 7 nights. The data has been acquired as log files for each night then we have merged all logs to create our dataset.

The size of the dataset is around 320 MG. It counts of about 6 Millions of points in the format of {*timestamp, x, z, y, EDA*}.

¹Robert Lawton - Own work

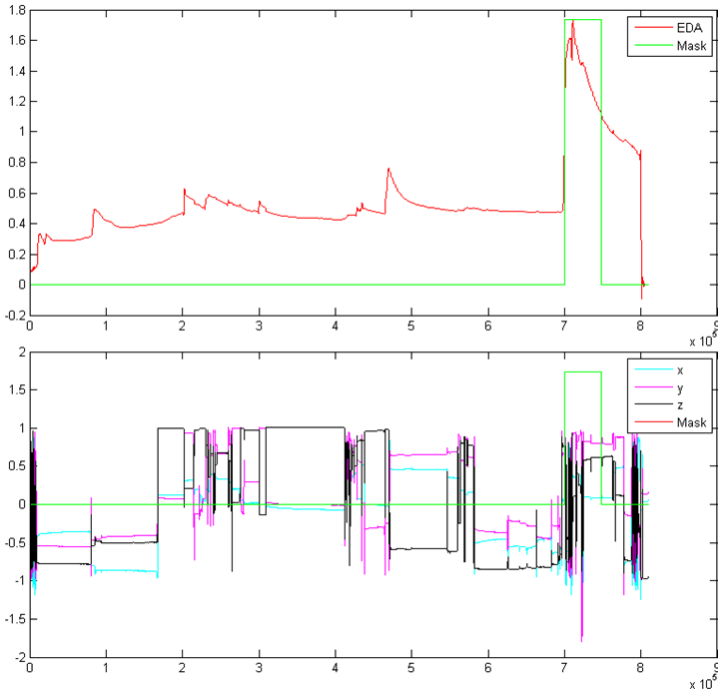


Fig. 2. (a) EDA Signals - (b) Acceleration Signals

Row ID	D niff	D SD	D Mean	S Class
Row297	0.001	-0.003	0	norm
Row298	0.002	-0	0.001	norm
Row299	0	-0.001	0.001	norm
Row300	0	-0.001	0.001	norm
Row301	0.002	0.001	0.001	norm
Row302	0	0.001	0	norm
Row303	0	0.001	0	norm
Row304	0	0.002	0.001	norm
Row305	0.001	0.001	0.001	norm
Row306	0	0.001	0.001	norm
Row307	0.001	0.001	0.002	norm
Row308	0.005	-0.004	0.005	norm
Row309	0.001	-0.002	0.004	anorm
Row310	0.002	0	0.007	anorm
Row311	0.031	0.031	0.059	anorm
Row312	0.031	0.031	0.002	anorm

Fig. 3. Training Data-Set of the Deep Neural Network

From the whole dataset, we have extracted 80% for the definition of the training set and the 20% for the testing set. The TD has been used to train both the deep neural network (DNN) [8] and conventional neural network (CNN) [8].

A. Deep Neural Network

The first step is to define a suitable training dataset (TD) from the training set for the DNN.

In our scenario the TD is composed of a set of vector of features f_i extracted from a temporal windows w_i , with $i = 1...N$.

We define a *temporal windows* (w_i) as a piece of the raw signals with a duration time of 10 seconds.

The selected features are: the *mean*, *standard deviation* and the *difference* $|mean(w_i) - mean(w_{i-1})|$.

For each features we have assigned the correct class: { *Normal Sleep* (N), *Anomalous Sleep* (A) }.

In order to do that, we have reused the results obtained from our previous works [6] in which we have recognized the sleep states of the temporal windows by means of threshold-based approach.

Figure 3 shows a piece of the training dataset that we have created. Each line is a vector of futures f_i .

The second step is the building of the DNN. Figure 4 shows a generic structure of a neural network.

Basically, a generic neural network is formed in three layers, called the input layer, hidden layer, and output layer. Each layer consists of one or more nodes, represented in this diagram by the small circle.

The nodes of the input layer receive a single value on their input and duplicate the value to their output.

The hidden layers are in charge to get the data and analyzed

Input layer Hidden layers Output layer

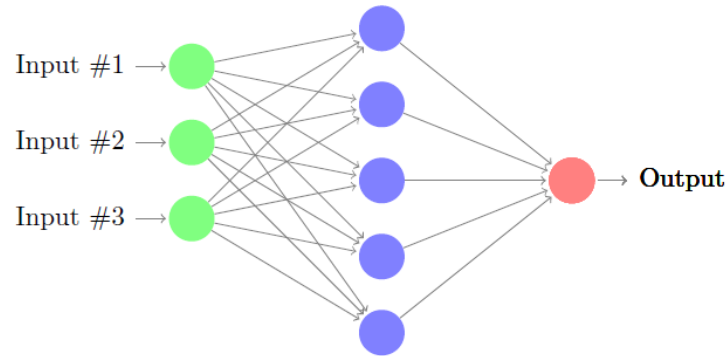


Fig. 4. Generic Structure of a Neural Network

them and provide results to the next layer. The output layers show the results of the learning process (e.g. a prediction/classification).

In our paper, the numbers of the nodes of the output layers are two ({ *Normal Sleep* (N), *Anomalous Sleep* (A) }). The size of the input layer is equal to the size of the features vectors.

The number of the units of each hidden layer and the number of the hidden layers are two hyperparameters that we have considered for the tuning of the DNN.

In order to find the best hyper-parameters setting, we have performed a set of experiments changing the values of the hyper-parameters.

We have tested the number of hidden layer in a range from 2 to 4 layers.

In the same way, we have evaluated the number of the units

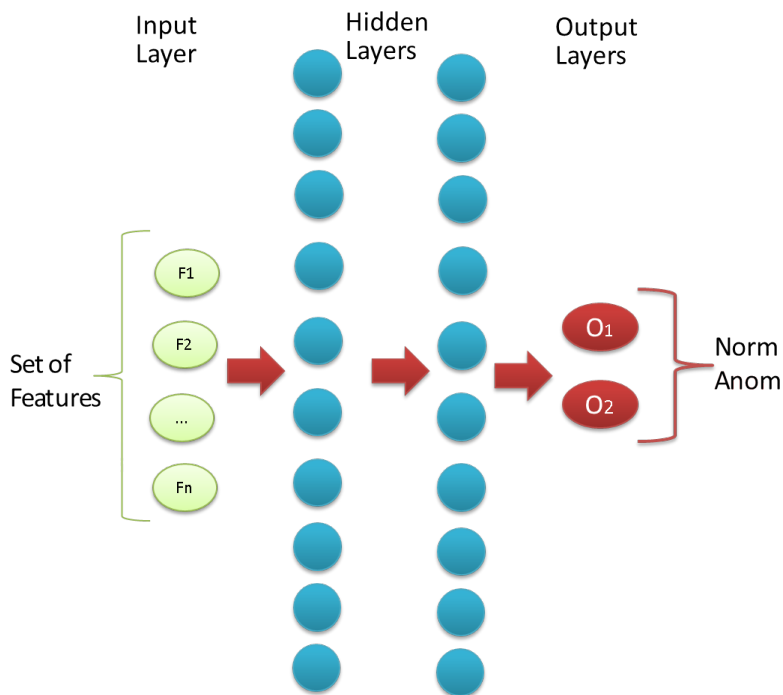


Fig. 5. Structure of the selected Deep Neural Network

for each layer in a range from 5 to 20 units.

The configuration that given the best performance in terms of accuracy was with 2 hidden layers with 10 units for each layer, Figure 5.

Other configurations with a higher numbers of both layers and units have produced the same results of the selected one.

B. Convolution Neural Network

A CNN structure is formed on tree basic type of layers: convolutional layers (CL), polling (P) and fully-connected (FC) layers.

The convolutional layers are in charge to perform the features extraction stage. Each input of the unit in this layer is connected to a local receptive file of the previous one.

The pooling layers perform the features reducing from the results of the previous CL.

The fully-connected layer Finally takes all output/neurons in the previous layer and connects it to every single neuron it has as in a classic neural network, an overall view of the generic structure of a CNN is shown in figure 6.

In our experiment we have adopted as pooling function the max-pool, in other words, for each temporal windows, the network considers only the point with max values from the output of the CL.

The hyper-parameters take in account for our experiments are:

- Learning rate
- Number of Convolutional Layers
- Number of the units of Convolutional Layers
- Number of the Fully-connected Layers
- Dropout

The *Learning rate* is a training parameter that controls the size of the steps of the changes during the learning process of the

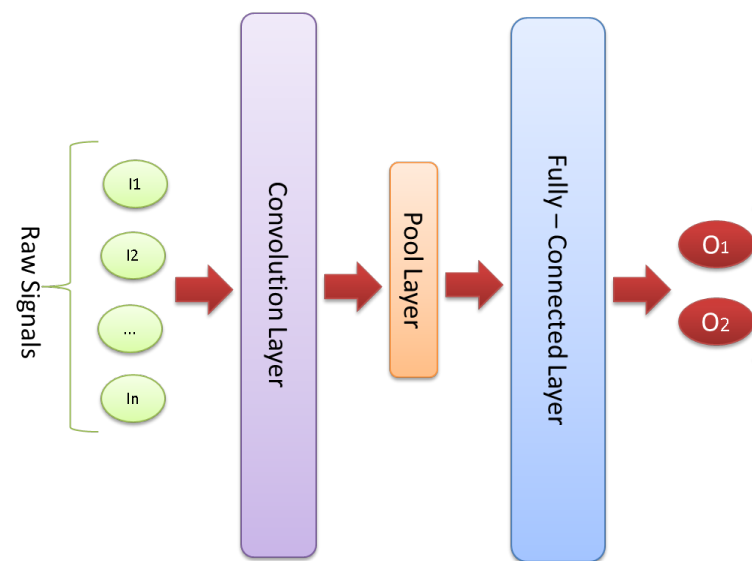


Fig. 6. Generic Structure of a Convolutional Neural Network

training algorithm (e.g Stochastic Gradient Descent) [16].

The *Dropout* is a regularization technique for reducing over-fitting in neural networks by preventing complex co-adaptations on training data [17].

In order to find the best configuration for the hyper-parameters of the CNN, we have performed a set of experiments by combining them and changing their values.

The range of the values was:

- Learning rate $\in \{0.01, 0.001, 0.0001\}$
- Number of Convolutional Layers $\in \{1, 2, 3\}$
- Number of the units of Convolutional Layers $\in \{1, 2, 3\}$
- Number of the Fully-connected Layers $\in \{1, 2, 3\}$
- Dropout $\{YES, NO\}$

The *deeper* configuration of our network reach a number of levels composed of 3 level of CL, 3 levels of FC and 1 level of dropout, for an amount of 7 levels.

For that configuration, we have reached a learning time around of 24 hours.

It is important to highlight a different between DNN and CNN about how they have been trained.

In CNN experiments we have not used the TD defined for the DNN, instead, we have used the raw data of the training set for the training of the CNN.

The reason of that is because we want to use one of the most important properties of the CNN, the capability of finding local connections between data [18].

For this reason, the input size of the CNN is equal to the temporal windows ws of the training set, the length of the the ws is 10 seconds with a sampling rate of 32 Hz(f_0) so the number of input of the first convolution level (CL) is to 320 inputs.

The number of output of each CL is set by dividing its number of input by 2.

We have applied the same procedure for the setting the number of output of the FC layers with a number of input of the first

TD	Accuracy DNN	Accuracy CNN
XYZ	89%	84%
EDA	50%	80%
XYZ + EDA	18%	84%

Fig. 7. Accuracy Performance

layer set to 1028 neurons.

After the training of the networks, we have used the test set for the evaluation of the performance of the two algorithms. For the DNN we have created a set of vector features from a temporal window extracted from the test set, for the CNN the have used directly the data of the test set.

IV. RESULTS

We report the results of the experiments in the Figure 7. We have defined three kinds of training data (TD_i) from the raw data, each one has been created by the biomedical signals acquired.

That motivated in order to evaluate the response of the algorithm to a different type of signals, XYZ, EDA, and XYZ+EDA. In details:

- 1) TD1: Only signals related to the patient's movements (XYZ)
- 2) TD2: Only signal related to the patient's Stress level (EDA)
- 3) TD3: All signals (XYZ + EDA)

We have submitted each type of training data to both CNN and DNN.

As we can see from the results, Figure 7, we have reached a discrete accuracy for XYZ signal with both kinds of the algorithm.

This result shows that both networks are able to recognize an anomalous sleep of stage by analyzing the patient's movements and taking into account only one sensor.

About the EDA signal, the results are very different, the CNN has reached an accuracy at 80% despite the 50% of DNN. A possible motivation of that should be that the EDA signal is not well-characterized unlike the movements so an approach based on features extraction should not be described well this kind of signal for the purpose of our work.

The CNN look like able to find some hidden correlations among the raw data that allow it to both learn better the structure of EDA signal and reach a higher accuracy.

In the last experiments, we have combined both the EDA and the XYZ signals.

The result of the DNN is quite low, 18%, despite the CNN that show a good accuracy, 80%.

The motivation behind this different results is still under investigation.

V. CONCLUSION

In this paper, we have evaluated a fist trial of experiments for the application of Deep Learning for the classification of

sleep disorders in a patient with Alzheimer's Disease. We have evaluated two type of algorithm: Deep Neural Network and Convolution Neural Network.

We have monitored one patient for one week and we have created a data set for both training and testing process.

The preliminary results look like shown that CNN performs a better evaluation for the classification of sleep anomaly stages by using both XYZ signal and EDA. As future, we have several issues to face such as:

- increasing the number of the monitored patient
- evaluating another training dataset by changing type of features
- evaluating the application of the recurrent neural network.
- deploying more sensors both on the patient and into the monitoring environment
- evaluating the reliability and dependability of the sensors by using approach as [19], [20].

ACKNOWLEDGMENT

This work is fully supported by the eAsy inteLLigent service Platform for Healthy Ageing (ALPHA) Project.

REFERENCES

- [1] E. A. Hahn, H.-X. Wang, R. Andel, and L. Fratiglioni, "A change in sleep pattern may predict alzheimer disease," *The American Journal of Geriatric Psychiatry*, vol. 22, no. 11, pp. 1262 – 1271, 2014, physical Comorbidity. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1064748113002339>
- [2] J. Cedernaes, R. S. Osorio, A. W. Varga, K. Kam, H. B. Schith, and C. Benedict, "Candidate mechanisms underlying the association between sleep-wake disruptions and alzheimer's disease," *Sleep Medicine Reviews*, vol. 31, pp. 102 – 111, 2017. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1087079216000186>
- [3] J. E. Smith and J. M. Tolson, "Recognition, diagnosis, and treatment of restless legs syndrome," *Journal of the American Academy of Nurse Practitioners*, vol. 20, no. 8, pp. 396–401, 2008. [Online]. Available: <http://dx.doi.org/10.1111/j.1745-7599.2008.00337.x>
- [4] A. Coronato and G. Paragliola, "A structured approach for the designing of safe aal applications," *Expert Systems with Applications*, vol. 85, pp. 1–13, 2017.
- [5] A. Coronato and G. De Pietro, "Situation awareness in applications of ambient assisted living for cognitive impaired people," *Mobile Networks and Applications*, pp. 1–10, 2013.
- [6] A. Coronato and G. Paragliola, "An approach for the evaluation of sleeping behaviors disorders in patients with cognitive diseases: A case study," in *2016 12th International Conference on Signal-Image Technology Internet-Based Systems (SITIS)*, Nov 2016, pp. 545–550.
- [7] "Empatica." [Online]. Available: <https://www.empatica.com/get-started-e4>
- [8] D. Rav, C. Wong, F. Deligianni, M. Berthelot, J. Andreu-Perez, B. Lo, and G. Z. Yang, "Deep learning for health informatics," *IEEE Journal of Biomedical and Health Informatics*, vol. 21, no. 1, pp. 4–21, Jan 2017.
- [9] F. Poree, A. Kachenoura, H. Gauvrit, C. Morvan, G. Carrault, and L. Senhadji, "Blind source separation for ambulatory sleep recording," *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 2, pp. 293–301, April 2006.
- [10] M. Z. Islam, K. M. T. Nahiyani, and M. A. Kiber, "A motion detection algorithm for video-polysomnography to diagnose sleep disorder," in *2015 18th International Conference on Computer and Information Technology (ICCI)*, Dec 2015, pp. 272–275.
- [11] A. E. Flores, J. E. Flores, H. Deshpande, J. A. Picazo, X. Xie, P. Franken, H. C. Heller, D. A. Grahn, and B. F. O'Hara, "Pattern recognition of sleep in rodents using piezoelectric signals generated by gross body movements," *IEEE Transactions on Biomedical Engineering*, vol. 54, no. 2, pp. 225–233, Feb 2007.
- [12] R. Prashanth, S. D. Roy, P. K. Mandal, and S. Ghosh, "Parkinson's disease detection using olfactory loss and rem sleep disorder features," in *2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Aug 2014, pp. 5764–5767.

- [13] J. Alves de Mesquita and P. Lopes de Melo, "Respiratory monitoring system based on the nasal pressure technique for the analysis of sleep breathing disorders: Reduction of static and dynamic errors, and comparisons with thermistors and pneumotachographs," *Review of Scientific Instruments*, vol. 75, no. 3, pp. 760–767, 2004. [Online]. Available: <http://scitation.aip.org/content/aip/journal/rsi/75/3/10.1063/1.1646734>
- [14] C. Occhiuzzi and G. Marrocco, "The rfid technology for neurosciences: Feasibility of limbs' monitoring in sleep diseases," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 1, pp. 37–43, Jan 2010.
- [15] J. Park, D. Kim, C. Yang, and H. Ko, "Svm based dynamic classifier for sleep disorder monitoring wearable device," in 2016 IEEE International Conference on Consumer Electronics (ICCE), Jan 2016, pp. 309–310.
- [16] Y. Bengio, "Practical recommendations for gradient-based training of deep architectures," *CoRR*, vol. abs/1206.5533, 2012. [Online]. Available: <http://arxiv.org/abs/1206.5533>
- [17] G. E. Hinton, N. Srivastava, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, "Improving neural networks by preventing co-adaptation of feature detectors," *CoRR*, vol. Abs/1207.0580, 2012. [Online]. Available: <http://arxiv.org/abs/1207.0580>
- [18] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.
- [19] A. Testa and A. Coronato, "A review of the methods for the dependability assessment of wsns: Towards a new approach." *Adhoc & Sensor Wireless Networks*, vol. 33, 2016.
- [20] A. Testa, M. Cinque, A. Coronato, G. De Pietro, and J. C. Augusto, "Heuristic strategies for assessing wireless sensor network resiliency: an event-based formal approach," *Journal of Heuristics*, vol. 21, no. 2, p. 145, 2015.

7th International Workshop on Advances in Semantic Information Retrieval

RECENT advances in semantic technologies form a solid basis for a variety of methods and instruments that support multimedia information retrieval, knowledge representation, discovery and analysis. They influence the way and form of representing documents in the memory of computers, approaches to analyze documents, techniques to mine and retrieve knowledge. The abundance of video, voice and speech data also raises new challenging problems to multimedia information retrieval systems.

We believe that our workshop will facilitate discussions of new research results in this area, and will serve as a meeting place for researchers from all over the world. Our aim is to create an atmosphere of friendship and cooperation for everyone, interested in computational linguistics and semantic information retrieval. The ASIR'17 workshop will continue to maintain high standards of quality and organization, set in the previous years. We welcome all the researchers, interested in semantic information retrieval, to join our event.

TOPICS

The workshop addresses semantic information retrieval theory and important matters, related to practical Web tools. The topics and areas include but not limited to:

- Domain-specific semantic applications.
- Evaluation methodologies for semantic search and retrieval.
- Models for document representation.
- Natural language semantic processing.
- Ontology for semantic information retrieval.
- Ontology alignment, mapping and merging.
- Query interfaces.
- Searching and ranking.
- Semantic multimedia retrieval.
- Visualization of retrieved results.

SECTION EDITORS

- **Klyuev, Vitaly**, University of Aizu, Japan
- **Mozgovoy, Maxim**, University of Aizu, Japan

REVIEWERS

- **Carrara, Massimiliano**, Universita di Padova, Italy
- **Dobrynin, Vladimir**, Saint Petersburg State University, Russia
- **Goczyła, Krzysztof**, Gdansk University of Technology, Poland
- **Haralambous, Yannis**, Institut Telecom - Telecom Bretagne, France
- **Homenda, Wladyslaw**, Warsaw University of Technology, Poland
- **Jin, Qun**, Waseda University, Japan
- **Lai, Cristian**, CRS4, Italy
- **Leonelli, Sabina**, University of Exeter, United Kingdom
- **Nalepa, Grzegorz J.**, AGH University of Science and Technology, Poland
- **Pyshkin, Evgeny**, University of Aizu, Japan
- **Shtykh, Roman**, CyberAgent Inc., Japan
- **Suárez-Figueroa, Mari Carmen**, Ontology Engineering Group, School of Computer Science at Universidad Politécnica de Madrid, Spain
- **Tadeusiewicz, Ryszard**, AGH University of Science and Technology, Poland
- **Vacura, Miroslav**, University of Economics, Czech Republic
- **Zadrozny, Sławomir**, Systems Research Institute of Polish Academy of Sciences, Poland
- **Ławrynowicz, Agnieszka**, Poznan University of Technology, Poland

FLOODS: A Succinct File System Structure

Daniel Peters*, Johannes Fischer†, Florian Thiel* and Jean-Pierre Seifert‡

*Physikalisch-Technische Bundesanstalt (PTB), Germany

Email: {daniel.peters, florian.thiel}@ptb.de

†Department of Computer Science, TU Dortmund, Germany

Email: johannes.fischer@cs.tu-dortmund.de

‡Security in Telecommunications, TU Berlin, Germany

Email: jpseifert@sec.t-labs.tu-berlin.de

Abstract—To spot malicious manipulation, remote attestation and maintenance for devices that are under legal control is very important. One example are measuring instruments, where the manufacturer and the market surveillance want to check if system integrity is preserved. In Europe, legal requirements state that a software identifier needs to be supplied/output by the device, which is often just a checksum over the files that are considered to be legally relevant for the measuring purpose. As measuring instruments and also other legally monitored devices are often small embedded systems, the need for a fast algorithm arises that creates a small file system list containing as much information as possible. In this paper, a new file system structure called FLOODS is explained that fulfills these requirements. The FLOODS uses theoretical optimal space to represent the file system structure, while it, nevertheless, enables fast file searches by names and also properties. For example, all files of a specific file type, e.g., pictures, movies, executables, etc., can be listed in $O(p \lg n)$ time, where p is the number of files of the specific file type searched for, and, where n represents the total number of file types in the system.

I. INTRODUCTION

IN MANY states, law obliges manufacturers of devices that are under legal control, to implement an easy procedure to output a software identifier. For example, measuring instruments under legal control, e.g., commodity meters for the supply of gas, water and electricity, etc., output these identifiers to show market surveillance agents that the approved software is still running on the device and system integrity is preserved. Hereby, the agents check the devices on sidein predefined intervals, e.g. every two years. Often, just a checksum over the legally relevant files is calculated. As measuring instruments and also other legally supervised devices are often powerful embedded instruments, it can be inferred that more efficient algorithms can be implemented that enhance the checksum or hash value with additional information, like the file system structure. Additionally, data exchange between devices over the internet has become an important aspect, nowadays. In the era of the Internet of Things (IoT), the number of these devices will, according to Gartner [46], exceed 25 billion in the year 2020. As storage units have become smaller and cheaper, these devices can already save millions of files. Considering that in the future the automatic data exchange between these devices will blossom, the creation of a small data structure listing all the files on a device is handy. Despite being small, this data structure should also be quickly traversable. It should list as much information about a file as possible to check, for

example, the name, the format, the size, and the checksum.

This paper describes such a data structure which makes use of succinct approaches to store trees. In this structure, a fast file search is made possible by using space-efficient algorithms to store the file names. Hence, the data structure is not only usable as a file list, but can easily be used as the fundamental structure for a read-only file system in which files can be located and listed efficiently.

A. Outline

The paper is structured as follows: In Section I, an introduction about the topic will be given, outlining the importance and usability of a succinct file system structure. In Section II, an overview of succinct data structures will be supplied, explaining important operations like *rank*- and *select*, which are needed to traverse many succinct data structures, one such data structure is the "Level Order Unary Degree Sequence" (LOUDS). The "File system Level Order Unary Degree Sequence" (FLOODS), which is based on the LOUDS, will be explained in detail in Section III. Afterwards, practical tests in Section IV will show the efficiency of the FLOODS by comparing it with the *locate* database of UNIX systems. At the end, before the conclusion in Section VI, a discussion is given in Section V which describes where the FLOODS can be used and how file modifications can be handled.

II. SUCCINCT DATA STRUCTURES

In this section existing data structures are presented that form the basis of the new succinct file system representation. All the results are in the word-RAM model of computation, i.e. the machine consists of words of width w bits that can be manipulated in $O(1)$ time by a standard set of logical and arithmetic operations, and the problem size n is not larger than $O(2^w)$.

In the past two decades, succinct data structures have been one of the key contributions to the algorithmic community. The aim of these structures is to represent objects from a universe of size u in information-theoretical optimal space $\lg u$ bits of space (function \lg denotes the binary logarithm throughout this paper). Additionally, fast operations should be supported, ideally in time no worse than with a "conventional" data structure for the object. Usually, a space overhead of no more than $o(\lg u)$ bits space arises for this property.

Ordered trees are just one example, where succinct data structures yield good result. Hereby, with n nodes we have a universe of size $u \approx 4^n$. In 1989, Jacobson first described such a tree representation that used only $10n + o(n)$ bits, while supporting the most common navigational operations in $O(\lg n)$ time [29]. With time, new succinct data structure for trees where developed that use the optimal $2n + o(n)$ bits and optimal $O(1)$ navigation time, e.g. [39]. A conventional, pointer-based data structure, for example, requires $\Theta(n \lg n)$ bits.

There are many more examples of succinct data structures: bit-vectors [41], dictionaries [40], binary relations [3], permutations [37], suffix trees [45], etc. In nearly all cases, attempts were made at practical implementations, with successful results [20], [24], [31].

A. Rank and Select

Many succinct data structures make use of two fundamental operations, called *rank*- and *select*. In this paper, these operations on S , with $S[1, n]$ being a *bit-string* of length n , are defined as follows:

- $\text{rank}_1(S, i)$ gives the number of 1's in the prefix $S[1, i]$
- $\text{select}_1(S, i)$ gives the position of the i 'th 1 in S , reading S from left to right ($1 \leq i \leq n$)

To give an example, in a string $S = 01001$ of size 5, where position 1 denotes the leftmost bit, $\text{rank}_1(S, 3) = 1$, and $\text{select}_1(S, 2) = 5$. Operations $\text{rank}_0(S, i)$ and $\text{select}_0(S, i)$ are defined similarly for 0-bits. S can be represented in $n + o(n)$ bits such that *rank*- and *select*-operations are supported in $O(1)$ time [39].

The approach used to achieve this is to divide the bit-string S into blocks of fixed size, e.g. 64 bit, and store the number of ones before the blocks. These blocks can be combined into bigger blocks, e.g. of size 4096 bits, often called super-blocks, which again store the number of ones at the position in front of each super-block. After each super-block the number of ones for the upcoming smaller block is reset to 0. Every super-block needs $\lg n$ bits and with the example of 4096 bit size super-blocks, each small block needs only $\lg(4096) = 12$ bits to store the number of ones till this position. $\text{rank}_1(S, i)$ can then be performed by accessing the blocks and adding them together. Getting the number of ones inside a block is done by bit-operations and/or table-lookups to speed up the process. The approach for $\text{select}_1(S, i)$ is similar but a little bit trickier, a nice description can be found in [9], where a three level directory structure is used.

B. Storing Trees Succinctly

There are several ways to represent an ordered tree with n nodes using $2n$ bits. The best known are the "level order unary degree sequence" (LOUDS), the "balanced parantheses" (BP) and the "depth first unary degree sequence" (DFUDS) [5], [29], [38]. A comparison of these structures is depicted in Figure 1.

The LOUDS is formed by performing a breadth-first traversal (BFT) on the tree, starting with an artificial super-root that

is added in front of the real root node and connected to it. At every step of the BFT $1^d 0$ is added to the LOUDS for each node, with d being the number of children of the respective node.

The BP and DFUDS use the depth-first traversal (DFT) for their construction. The BP is constructed as follows: when the DFT descends a level, an opening parenthesis is written, and when it ascends, a closing one is written.

The DFUDS combines the BP and the LOUDS. Hereby, when the DFT descends to a node, d open parentheses are written out, with d being the number of the children of that node. After the node traversal a closing parenthesis is written out. Like in the LOUDS, an opening parentheses is added at the beginning, similar to the artificial super-root.

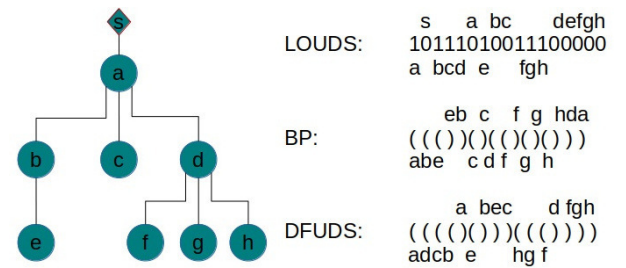


Fig. 1: Comparison between LOUDS, BP und DFUDS (s is the artificial super-root)

For the LOUDS only *rank*- and *select* is needed to enhance the data structure with navigational operations. The BP and the DFUDS need some more structures:

- $\text{enclose}(S, p)$: Finds the pair of parentheses, which encloses the open parentheses at position p most tightly and returns the position of the open parenthesis of the pair of parentheses.
- $\text{findclose}(S, p)$: Returns the position of the closing parentheses which belongs to the open parentheses at position p .
- $\text{findopen}(S, p)$: Returns the position of the open parentheses which belongs to the closing parentheses at position p .

All these functions can be implemented in $O(1)$ time with $o(n)$ space, with very small and fast practical data structures, see, e.g [19]. As can be noticed, all succinct data structures for trees [5], [10], [14], [29], [38] must have the freedom to fix a particular naming for the nodes; natural such namings are post- or pre-order [5], [29], [38], in-order [10], and level-order [29].

As the LOUDS is easier to implement and needs only *rank*- and *select*, it practically also uses less space. Therefore, we think the best choice is to use it as the fundamental structure of the file system structure explained in Section III.

Augmenting the LOUDS with *rank*- and *select* results in the total space of $2n + o(n)$ bits, where the basic navigational operations on trees are simulated in $O(1)$ time: Getting the parent of node i ($1 \leq i \leq n$) is done by jumping to the

position y of the i 'th 1-bit in S by $y = \text{select}_1(S, i)$, and then by counting the number j of 0's that are present before y , with $j = \text{rank}_0(S, y)$. The resulting j represents the level-order number of the parent of i . Listing the children of i is done by going to the position x of the i 'th 0-bit in S by $x = \text{select}_0(S, i)$, and then iterating over the positions $x + 1, x + 2, \dots$, as long as the corresponding bit is '1'. For each such position $x + k$ with $S[x + k] = 1$, the level-order numbers of i 's children are $\text{rank}_1(S, x) + k$, which can be simplified to $x - i + k + 1$.

To give an example, we look more close at Fig. 1. Here, the LOUDS is $S = 10111010011100000$, with the corresponding tree depicted at the left hand side of the figure. Now, to get the children of the fourth node (in Fig. 1 denoted as d), we calculate the position of the first child of d in S : $x_1 = \text{select}_0(S, 4) + 1 = 10$. We then check if $S[x_1] = 1$ and if so ($S[10] = 1$) we increment the position by one until we arrive at a 0. In our example until position 13, i.e. positions 10, 11, 12 are the positions of the children of node 4 (d). To convert the positions to the tree numbers, we then have to calculate $c_1 = \text{rank}_1(S, 10) = 6$ (f in alphabetical numbering as shown in Fig. 1), $c_1 = \text{rank}_1(S, 10) = 7$ (g), and $c_1 = \text{rank}_1(S, 10) = 8$ (h). For a parent, let us take node the third node as an example (in Fig. 1 denoted as c). Here, $y = \text{select}_1(S, 3) = 4$ is the position of the node in the LOUDS, and with $j = \text{rank}_0(S, 4) = 1$, we get 1 as a result (a).

C. Wavelet Trees

The operations *rank*- and *select* have been extended to sequences over larger alphabets, at the cost of slight slowdowns in the running times [4], [21]. In this section a practical approach is discussed, called *wavelet tree* [23]. A wavelet tree is constructed as follows: First each character c in a text S is assigned to exactly one bit (a 0 or a 1). The root node v_1 is situated on the first level and contains the bit-vector B_1 and the actual text $S_1 = S$. Now the tree is built recursively: If a node v contains a text S_v that has at least two different characters, then two child nodes v_l and v_r are created. All characters which are marked with a 0 go to the left node and all other characters go to the right node. Note that at the end the S_v 's of every node are not saved, only their bit vectors B_v with the *rank*- and *select* data structures, and the mappings "c to leaf" and "leaf to c". If a balanced wavelet tree is constructed, in which the first half of a node's alphabet is written into the left child and the other half into the right one, the mappings from "c to leaf" and from "leaf to c" do not need to be stored, and the tree can still be easily traversed. Figure 2 shows such a balanced wavelet tree for $S = 303302013032012010010$.

The advantage of these wavelet trees is that $\text{select}_c(S, i)$, $\text{rank}_c(S, j)$ and $\text{access}(j)$ queries for an alphabet of size σ can be answered in $O(\lg \sigma)$ time for every character c in S and position j in S , while using only $n \lg \sigma + o(n \lg \sigma)$ space.

To give an example, we look at Fig. 2. Here, $\text{rank}_3(S_1, 6)$ can be calculated as follows. We know that 3 is in the second half of our alphabet (0, 1 are represented as a 0 in B_1 , and the numbers 2 and 3 are represented as a 1). So first,

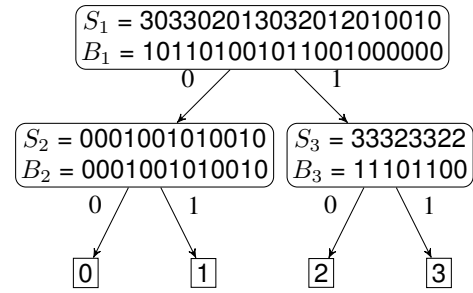


Fig. 2: Illustration of a balanced wavelet tree.

$\text{rank}_1(B_1, 6) = 4$ and then $\text{rank}_1(B_3, 4) = 3$ (here again 3 is represented as a 1 in B_2 because it is in the second half of the alphabet, and 2 in the first), meaning in total $\text{rank}_3(S_1, 6) = 3$. For select a similar procedure is being used only that now we start from the leaves. To calculate $\text{select}_1(S_1, 2)$, we know that 1 is represented by a 0 in B_1 and as a 1 in B_2 . Hence, we get $\text{select}_1(B_2, 2) = 7$, and afterwards $\text{select}_0(B_1, 7) = 14$, so the result is $\text{select}_1(S_1, 2) = 14$.

III. FLOODS

An approach that is also based on the LOUDS to store tree-like graphs, which file systems with links can be regarded as, is explained in [16]. This method was developed primarily for storing phylogenetic networks (phylogenetic networks are used in biology to express relationships between species). The structure consists of a trit (ternary digit) variant to store the enhanced LOUDS, which is rather not suitable for file systems, because one can only differentiate between two types of files, e.g., links and regular files (the 0s in the trit-variant are used to end the children listing of a node as in the LOUDS). In this section, a new version called FLOODS ("File system Level Order Unary Degree Sequence") is described, which makes use of the wavelet tree presentation described in Section II-C. Therefore, files can be divided into more than two types, e.g. the types listed in Figure 3:

- regular files
- directories
- links (hard-, soft)
- block-oriented device
- char-oriented device

This list can be expanded, e.g. to sockets, pipes, MIME types (pictures, videos, ...) etc., or shortened as needed.

The FLOODS is created as follows: First a BFT at the root of the file system tree is started. For every node (file/folder) a predefined number representing the file type is appended to S . If the node is the first child of its father, a 1 is written to B , otherwise a 0. The array S can be created directly as a wavelet tree, when the number of file types t is known from the beginning; if not, it can be created later, after the complete BFT run.

Additionally, the file/folder names are successively written to N , whereas B_n marks the beginning of a new file name by a 1. After a complete BFT S , B , N and B_n are created and

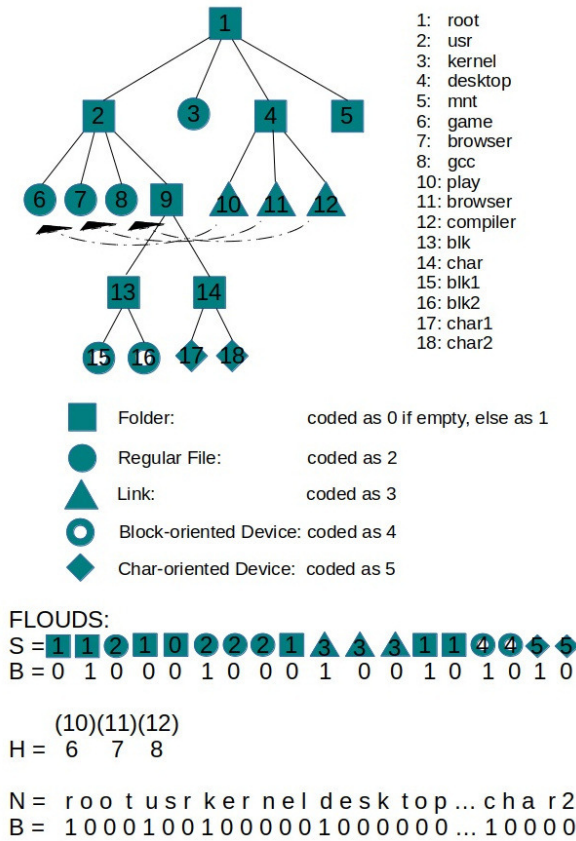


Fig. 3: File system structure FLOUDS, consisting of S , B , H , N and B_n .

the number of nodes n and the number of links l are known. This information can then be used to create the wavelet tree H , which is needed to retrieve the link address to the file. In total H requires $l \lg n + o(l \lg n)$ space. In H the FLOUDS numbers of the real files of the links are stored, in the order in which they were traversed by the BFT. Now, H can be used to check if a file is a link, and afterwards get the linked file, as described in the next section.

A. Navigating through the FLOUDS

With the help of S and B , a file system tree traversal can be done much like it in the LOUDS. Functions *parent* and *child* are as follows:

- $\text{child}(x, i) = \text{select}_1(B, \text{rank}_1(S; x)) + i - 1$, if $S[x] = 1$ and $i < \text{number of children}$
- $\text{parent}(x) = \text{select}_1(S, \text{rank}_1(B; x))$

For example, in Figure 3, the folder-entries of node 9 can be listed by first checking if node 9 is a folder $S[9] = 1$, and then getting its folder-number $f_n = \text{rank}_1(S; 9) = 4$. Afterwards, a jump to its first child is done, $\text{child}(9, 1) = \text{select}_1(B; 4) = 13$. All the children of node 9 are between the first and the last child l : $\text{child}(9, l) = \text{select}_1(B; 5) - 1 = 14$ (the position before encountering the next '1': $4 + 1 = 5$). So the folder-entries of node 9 are 13 and 14 (and $l = 2$).

The time complexity of outputting a child (folder entry) lies in $O(\lg t)$, with t being the number of file types in the FLOUDS, because all rank and select operations on B are supported in $O(1)$, and for S , which is saved in a wavelet tree format, in $O(\lg t)$.

The array H can be used to check if a node is a link (in the example from Figure 3: $S[n] = 3$) or if a file is referenced by links, and where these links are situated in the file system tree, by using the wavelet tree of H :

- $\text{getLink}(n, i) = \text{select}_3(S; \text{select}_n(H; i))$
- $\text{getOrig}(n) = H[\text{rank}_3(S; n)]$, if $S[n] = 3$

Looking again at the example of Figure 3: the first link that points to node 7 is $\text{getLink}(7, 1) = \text{select}_3(S; \text{select}_7(H; 1)) = 11$; and the file-number (node) 12 points to is $\text{getOrig}(12) = H[\text{rank}_3(S; 12)] = 8$. Hence, the FLOUDS also enables to print out its direct parent directory, and additionally, if it is a link or has links pointing to it, the parent directories the other links are stored in. Hereby, the time complexity depends on the wavelet tree of H and S to find the files, so summing up, listing all parent folders of a file including the parent folders of its links, is in $O(a * (\lg l + \lg t))$, with l being the number of all original files that have links, t the number of total file types in the whole file system, and a the actual number of links of the searched file.

Additionally, with the help of *rank*- and *select*, the following functions are directly executable:

- Getting the number of files in a folder and listing them.
- Getting the number of files of a specific file-type in a folder and listing them.

For example, if every file is assigned a MIME-type number, all pictures in the file system can be listed efficiently.

B. Efficiently Storing File Names

A simple method to find files fast can be achieved by sorting the folder entries in alphabetical order. Hereby, the prefix of a file name in a folder can be found by a binary search.

A more efficient search that also finds substrings of file names can be achieved by applying 2-Way dictionaries. An example would be using the Burrows-Wheeler Transform (BWT) [8] with Run-Length Encoding. Such a method is described in [15], for example. Hereby, substrings can be found efficiently, and afterwards be mapped to their FLOUDS numbers, or the file names can be read out via the FLOUDS numbers, respectively.

Another method that aims at compression, is described in [2]. There, the Lempel-Ziv algorithm 78 (LZ78 [47]) is altered in a way that makes locating prefixes possible. The LZ78 compression algorithm for a string $S[1, n]$ proceeds by parsing S from left to right. Hereby, S is divided into blocks that are one-letter extensions of previously parsed substrings. The set of current blocks is called the phrase dictionary D . The dictionary D is prefix-closed and represented with a trie (the LZ-trie), which is stored in [2] with some enhancements to achieve look-up and access support. The method is good for checking the integrity of file system structures, because finding

substrings of file names is not really needed (the exact file name is known a priori).

C. Integrity checking

There are several variations to check file system integrity on request:

- 1) The FLOUDS is signed and transferred with the file names.
- 2) The FLOUDS is newly created and while traversing the file system tree, a hash value of each file is calculated. These hash values are written into a hash array of size n and transmitted together with the FLOUDS and the file names.
- 3) To save space, the file name list can be omitted. The file names can just be included in the computation of the hash values, mentioned in point 2.
- 4) Only a predefined number of files are hashed to save even more space.
- 5) Only one hash value over the entire structure is calculated and transmitted.

The fifth method requires the least amount of space, because only a hash value needs to be transmitted. This value can, for example, be displayed on the device's display. If the hash has an unexpected value, one of the other four methods can be executed to check, how the file system structure has changed and which files have been altered.

The used hash algorithm should be as collision-free as possible. Still, it can be freely chosen, for example from a simple checksum like CRC16, to secure hashing algorithms such as SHA-2, depending on performance, space or safety demands.

IV. PRACTICAL RESULTS

The aim of this section is to show the practicality of our approach by comparing it with a well known database for Unix systems, which the *locate* command uses to efficiently find files.

For our test we used the succinct libraries <https://github.com/ot/succinct> and <https://github.com/simongog/sdsl>, which have well-tuned succinct data structure implementations (other sources are [1], [18]). Our machine was equipped with an Intel Core i7@2.2GHz and 8GB of RAM, running under Ubuntu 14.04.

Table I shows the sizes of the *mlocate* database, which in Unix systems is normally situated at `/var/lib/mlocate/mlocate.db`, the size of the FLOUDS with the file names just stored in plain text, and the lzFLOUDS with the file names stored by the LZ78 method [2] described in Section III-B.

We used 4 different file lists for comparison:

- 1) *buildroot*: *buildroot* (<http://buildroot.uclibc.org/>) is a tool to generate embedded Linux systems, the file system we generated contained 435 nodes (files/folders/link etc.).
- 2) *linux_src*: The Linux 4.2 Kernel source tree containing 54 171 nodes.

- 3) *comp1*: A small file system of a desktop computer containing 333 854 nodes.
- 4) *comp2*: A bigger file system of another desktop computer with 1 853 354 nodes.

TABLE I: Comparison of sizes in MB: 1. *buildroot*, 2. *linux_src*, 3. *comp1*, 4. *comp2*.

F	<i>mlocate</i>	FLOUDS	lzFLOUDS
1.	0.004	0.003	0.002
2.	0.957	0.625	0.218
3.	7.722	4.964	1.932
4.	42.876	22.928	9.141

The second table, Table II, compares the running times to find a file name. Hereby, the LZ78 variant of the FLOUDS searched for exact matches, whereas the other two searched for substrings. We averaged the running times over 100 tests, searching for random strings.

TABLE II: Comparison of running times in sec: Legend as in Table I.

F	<i>mlocate</i>	FLOUDS	lzFLOUDS
1.	0.004	0.027	$8 * 10^{-6}$
2.	0.035	0.105	$10 * 10^{-6}$
3.	0.381	0.565	$9 * 10^{-6}$
4.	0.823	9.854	$12 * 10^{-6}$

It can be observed that the naive FLOUDS representation is already around 40% smaller than the *mlocate* database. Still the running times for file-systems with many files are up to 12 times slower. On the other hand, the lzFLOUDS is some magnitudes faster than the other structures. The drawback of the lzFLOUDS is that it can only be used to find prefixes, and in our tests it just output a result, if the exact match was found. We think that this is enough, if the FLOUDS is used for integrity checking, because the exact file names should be known.

V. DISCUSSION

Succinct data structures perform very well on static objects and not that well on dynamic ones. The same applies to the FLOUDS, hence it is better suited for a read-only file system. For many embedded devices this poses no restriction, because mostly they are put in commission to fulfil only a certain scope; changes to the file system structure are often not allowed and would be a sign of malicious manipulation. However, if changes are to be made, the FLOUDS needs to be rebuilt. A fast rebuild can be easily achieved if the names are not compressed and saved in plain form. For the other representations, the file name string needs to be completely rebuilt, which can be slow. Still, dynamic succinct data structures exist that can be used to this end, e.g., [34].

Figure 4 shows how the file system manager should be separated from the computing component to hinder malicious applications from tampering with files if file integrity is an

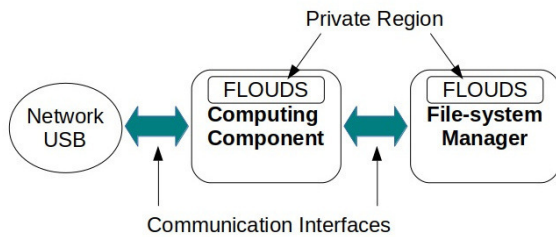


Fig. 4: Separating the file system Manager

issue. These components can be separate devices, where the file system component is at a secure location. Hereby, the computing component could have a copy of the FLOUDS in its internal storage, to speed up locating files. If a file is needed, the FLOUDS-number and the number of requested bytes can be sent to the file system manager, which then answers the request. This communication can be encrypted if an open network is used for communication. In the same manner, an entitled entity can check the integrity of the file system by just sending a request to the computing component, which in turn gets the FLOUDS encrypted with the private key of the file system manager. Afterwards, it sends this encrypted FLOUDS back to the entitled authority. After decrypting it with the public key of the file system component, the entitled authority can make sure that the computing component did not manipulate the FLOUDS-file (assuming of course that the private key of the file system manager is not known by the computing component).

Another approach is software-separation through virtualization. There are some papers that come to the conclusion that the microkernel approach for virtualization is recommended to construct secure systems [26]–[28], [33], [35], [42]. A concrete modular system architectures is described in [43], which yields good results also for embedded devices. It is based on virtualization by dividing critical parts of software from non-critical ones through virtual machines.

Another area of application for the FLOUDS is to use it as the fundamental structure of a whole file system. A possible approach would be to combine it with a read-only, compressed file system like squashFS (<http://squashfs.sourceforge.net/>). The idea is to use the FLOUDS numbers of the nodes to represent the block numbers, which in turn point to compressed blocks. Nevertheless, if compression is not that important, the FLOUDS needs to be evaluated against a dynamic file system, e.g., based on the B^c -tree, because these show good results for locating files and have fast write operations [11], [30].

VI. CONCLUSION

In this paper, a flexible file list structure called FLOUDS was presented. This structure was explained in detail to show that it can be used in many ways. Firstly, it is well suited for embedded devices that need to be validated for integrity in commission, or which want to exchange file lists. Secondly, it can be used as the groundwork for a read-only file system,

which uses as little space as possible. Lastly, it can be used to efficiently find and list files by using succinct data structures for trees and 2-way dictionaries. For the latter, the FLOUDS was evaluated by comparing it to another file name database, which is used in Unix systems by the *locate* command. These tests show that the FLOUDS stores more information, is smaller, and for integrity checking also faster.

REFERENCES

- [1] D. Arroyuelo, R. Cánovas, G. Navarro, and K. Sadakane. Succinct trees in practice. In *Proc. ALENEX*, pages 84–97. SIAM, 2010. <https://doi.org/10.1137/1.9781611972900.9>
- [2] J. Arz and J. Fischer. LZ-Compressed String Dictionaries. In *Data Compression Conference (DCC)*, pages 322 – 331, 2014. <https://doi.org/10.1109/DCC.2014.36>
- [3] J. Barbay, F. Claude, and G. Navarro. Compact rich-functional binary relation representations. In *Proc. LATIN*, volume 6034 of *LNCS*, pages 170–183. Springer, 2010. https://doi.org/10.1007/978-3-642-12200-2_17
- [4] D. Belazzougui and G. Navarro. New lower and upper bounds for representing sequences. In *Proc. ESA*, volume 7501 of *LNCS*, pages 181–192. Springer, 2012. https://doi.org/10.1007/978-3-642-33090-2_17
- [5] D. Benoit, E. D. Demaine, J. I. Munro, R. Raman, V. Raman, and S. S. Rao. Representing trees of higher degree. *Algorithmica*, 43(4):275–292, 2005. <https://doi.org/10.1007/s00453-004-1146-6>
- [6] D. K. Blandford, G. E. Blelloch, and I. A. Kash. Compact representations of separable graphs. In *Proc. SODA*, pages 679–688. ACM/SIAM, 2003. <http://doi.acm.org/10.1145/644108.644219>
- [7] D. K. Blandford, G. E. Blelloch, and I. A. Kash. An experimental analysis of a compact graph representation. In *ALENEX/ANALC*, pages 49–61. SIAM, 2004. <https://doi.org/10.1109/BOD.2006.320815>
- [8] M. Burrows and D. Wheeler. A block sorting lossless data compression algorithm. Technical Report 124, Digital Equipment Corporation, 1994.
- [9] D. Clark. Compact Pat Trees. Phd Thesis presented to the University of Waterloo, Canada. 1996.
- [10] P. Davoodi, R. Raman, and S. R. Satti. Succinct representations of binary trees for range minimum queries. In *Proc. COCOON, LNCS*, pages 396–407. Springer, 2012. https://doi.org/10.1007/978-3-642-32241-9_34
- [11] J. Esmet, M. A. Bender, M. Farach-Colton, and B. C. Kuszmaul. The TokuFS streaming file system. In *Proceedings of the 4th USENIX Workshop on Hot Topics in Storage (HotStorage)*, 2012.
- [12] A. Farzan and J. Fischer. Compact representation of posets. In *Proc. ISAAC*, volume 7074 of *LNCS*, pages 302–311. Springer, 2011. https://doi.org/10.1007/978-3-642-25591-5_32
- [13] A. Farzan and J. I. Munro. Succinct representation of arbitrary graphs. In *Proc. ESA*, volume 5193 of *LNCS*, pages 393–404. Springer, 2008. https://doi.org/10.1007/978-3-540-87744-8_33
- [14] A. Farzan and J. I. Munro. A uniform approach towards succinct representation of trees. In *Proc. SWAT*, volume 5124 of *LNCS*, pages 173–184. Springer, 2008. https://doi.org/10.1007/978-3-540-69903-3_17
- [15] P. Ferragina and R. Venturini. The compressed permuterm index. In *ACM Trans. Algorithms* 7, 1, Article 10, 21 pages, 2010. <https://doi.org/10.1145/1277741.1277833>
- [16] J. Fischer and D. Peters. A Practical Succinct Data Structure for Tree-Like Graphs. In *WALCOM: Algorithms and Computation*, pages 65–76, Springer, 2015. https://doi.org/10.1007/978-3-319-15612-5_7
- [17] C. Gavoille and N. Hanusse. On compact encoding of pagenumber k graphs. *Discrete Mathematics & Theoretical Computer Science*, 10(3):23–34, 2008.
- [18] R. F. Geary, N. Rahman, R. Raman, and V. Raman. A simple optimal representation for balanced parentheses. *Theor. Comput. Sci.*, 368(3):231–246, 2006. https://doi.org/10.1007/978-3-540-27801-6_12
- [19] S. Gog and J. Fischer. Advantages of Shared Data Structures for Sequences of Balanced Parentheses. In *Proceedings of the 2010 Data Compression Conference (DCC'10)*, IEEE Press, pages 406–415, 2010. <http://doi.org/10.1109/DCC.2010.43>
- [20] S. Gog and E. Ohlebusch. Fast and lightweight LCP-array construction algorithms. In *Proc. ALENEX*, pages 25–34. SIAM, 2011. <http://dx.doi.org/10.1137/1.9781611972917.3>
- [21] A. Golyński, J. I. Munro, and S. S. Rao. Rank/select operations on large alphabets: a tool for text indexing. In *Proc. SODA*, pages 368–373. ACM/SIAM, 2006. <http://dx.doi.org/10.1145/1109557.1109599>

- [22] R. González, S. Grabowski, V. Mäkinen, and G. Navarro. Practical implementation of rank and select queries. In *Poster Proceedings Volume of 4th Workshop on Efficient and Experimental Algorithms (WEA)*, pages 27–38, Greece, 2005. CTI Press and Ellinika Grammata. http://dx.doi.org/10.1007/978-3-540-89097-3_18
- [23] R. Grossi, A. Gupta, and J. S. Vitter. High-order entropy-compressed text indexes. In *Proceedings of the 14th Annual SIAM/ACM Symposium on Discrete Algorithms (SODA)*, pages 841–850. 2003.
- [24] R. Grossi and G. Ottaviano. Design of practical succinct data structures for large data collections. In *Proc. SEA*, volume 7933 of *LNCS*, pages 5–17. Springer, 2013. http://dx.doi.org/10.1007/978-3-642-38527-8_3
- [25] Y. Gurevich, L. Stockmeyer, and U. Vishkin. Solving NP-hard problems on graphs that are almost trees and an application to facility location problems. *J. ACM*, 31(3):459–473, 1984.
- [26] G. Heiser. The Role of Virtualization in Embedded Systems. In *Proceedings of the 1st Workshop on Isolation and Integration in Embedded Systems*, pages 11–16, 2008. <https://doi.org/10.1145/1435458.1435461>
- [27] G. Heiser, V. Uhlig, and J. LeVasseur. Are Virtual-machine Monitors Microkernels Done Right? *SIGOPS Oper. Syst. Rev.* 40, 2006. <https://doi.org/10.1145/1113361.1113363>
- [28] M. Hohmuth, M. Peter, H. Härtig, J. S. Shapiro. Reducing TCB Size by Using Untrusted Components: Small Kernels Versus Virtual-machine Monitors. In *Proceedings of the 11th Workshop on ACM SIGOPS European Workshop*, Leuven, Belgium, pages 19–22, 2004. <https://doi.org/10.1145/1133572.1133615>
- [29] G. J. Jacobson. Space-efficient static trees and graphs. In *Proc. FOCS*, pages 549–554. IEEE Computer Society, 1989.
- [30] W. Jannen, J. Yuan, Y. Zhan, A. Akshintala, J. Esmet, Y. Jiao, A. Mittal, P. Pandey, P. Reddy, L. Walsh, M. Bender, M. Farach-Colton, R. Johnson, B. C. Kuszmaul, and D. E. Porter. BetrFS: A Right-Optimized Write-Optimized File System. In *13th USENIX Conference on File and Storage Technologies (FAST 15)*, pages 301–315, 2015. <https://doi.org/10.1145/2798729>
- [31] S. Joannou and R. Raman. Dynamizing succinct tree representations. In *Proc. SEA*, volume 7276 of *LNCS*, pages 224–235. Springer, 2012. https://doi.org/10.1007/978-3-642-30850-5_20
- [32] S. Kannan, M. Naor, and S. Rudich. Implicit representation of graphs. *SIAM J. Discrete Math.*, 5(4):596–603, 1992.
- [33] M. Lange, S. Liebergeld, A. Lackorzynski, A. Warg, and M. Peter. L4Android: A Generic Operating System Framework for Secure Smartphones. In *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, Chicago, IL, USA, pages 39–50, 2011. <https://doi.org/10.1145/2046614.2046623>
- [34] S. Lee, and K. Park. Dynamic Rank-Select Structures with Applications to Run-Length Encoded Texts. In *Lecture Notes in Computer Science 4580*, Springer, pages 95–106, 2007. https://doi.org/10.1007/978-3-540-73437-6_12
- [35] A. S. Liebergeld, M. Peter, and A. Lackorzynski. Towards Modular Security-Conscious Virtual Machines. In *Proceedings of the Twelfth Real-Time Linux Workshop*, Nairobi, Kenya, pages 25–27, 2010.
- [36] J. I. Munro. Tables. In *Proc. FSTTCS*, volume 1180 of *LNCS*, pages 37–42. Springer, 1996.
- [37] J. I. Munro, R. Raman, V. Raman, and S. S. Rao. Succinct representations of permutations. In *Proc. ICALP*, volume 2719 of *LNCS*, pages 345–356. Springer, 2003. https://doi.org/10.1007/3-540-45061-0_29
- [38] J. I. Munro and V. Raman. Succinct representation of balanced parentheses, static trees and planar graphs. In *Proc. FOCS*, pages 118–126. IEEE Computer Society, 1997.
- [39] J. I. Munro and V. Raman. Succinct representation of balanced parentheses and static trees. *SIAM J. Comput.*, 31(3):762–776, 2001. <https://doi.org/10.1109/SFCS.1997.646100>
- [40] R. Pagh. Low redundancy in static dictionaries with constant query time. *SIAM J. Comput.*, 31(2):353–363, 2001. <https://doi.org/10.1137/S0097539700369909>
- [41] M. Pătraşcu. Succincter. In *Proc. FOCS*, pages 305–313. IEEE Computer Society, 2008. <https://doi.org/10.1109/FOCS.2008.83>
- [42] M. Peter, H. Schild, A. Lackorzynski, and A. Warg. Virtual Machines Jailed: Virtualization in Systems with Small Trusted Computing Bases. In *Proceedings of the 1st EuroSys Workshop on Virtualization Technology for Dependable Systems*, Nuremberg, Germany, 2009. <https://doi.org/10.1145/1518684.1518688>
- [43] D. Peters, M. Peter, J.-P. Seifert, and F. Thiel. A Secure System Architecture for Measuring Instruments in Legal Metrology. In *MDPI Computers*, 4(2), 61 – 86, 2015. <https://doi.org/10.1109/I2MTC.2015.7151517>
- [44] R. Raman, V. Raman, and S. S. Rao. Succinct indexable dictionaries with applications to encoding k -ary trees and multisets. *ACM Transactions on Algorithms*, 3(4):Article No. 43, 2007. <https://doi.org/10.1145/1290672.1290680>
- [45] K. Sadakane. Compressed suffix trees with full functionality. *Theory Comput. Syst.*, 41(4):589–607, 2007. <https://doi.org/10.1007/s00224-006-1198-x>
- [46] A. Velosa, J. F. Hines, H. LeHong, E. Perkins, R. M. Satish. Predicts 2015: The Internet of Things. In <https://www.gartner.com/doc/2952822/predicts--internet-things>, 2014.
- [47] J. Ziv and A. Lempel. Compression of individual sequences via variable-rate coding. In *Information Theory, IEEE Transactions*, 24(5), pages 530–536, 1978.

11th Joint Agent-oriented Workshops in Synergy

MULTI-AGENT systems (MASs) provide powerful models for representing both real-world systems and applications with an appropriate degree of complexity and dynamics. Several research and industrial experiences have already shown that the use of MASs offers advantages in a wide range of application domains (e.g. financial, economic, social, logistic, chemical, engineering). When MASs represent software applications to be effectively delivered, they need to be validated and evaluated before their deployment and execution, thus methodologies that support validation and evaluation through simulation of the MAS under development are highly required. In other emerging areas (e.g. ACE, ACF), MASs are designed for representing systems at different levels of complexity through the use of autonomous, goal-driven and interacting entities organized into societies which exhibit emergent properties. The agent-based model of a system can then be executed to simulate the behavior of the complete system so that knowledge of the behaviors of the entities (micro-level) produce an understanding of the overall outcome at the system-level (macro-level). In both cases (MASs as software applications and MASs as models for the analysis of complex systems), simulation plays a crucial role that needs to be further investigated.

TOPICS

JAWS'17 aims at providing a forum for discussing recent advances in Engineering Complex Systems by exploiting Agent-Based Modeling and Simulation. In particular, the areas of interest are the following (although this list should not be considered as exclusive):

- Agent-based simulation techniques and methodologies
- Discrete-event simulation of Multi-Agent Systems
- Simulation as validation tool for the development process of MAS
- Agent-oriented methodologies incorporating simulation tools
- MAS simulation driven by formal models
- MAS simulation toolkits and frameworks
- Testing vs. simulation of MAS
- Industrial case studies based on MAS and simulation/testing
- Agent-based Modeling and Simulation (ABMS)
- Agent Computational Economics (ACE)
- Agent Computational Finance (ACF)
- Agent-based simulation of networked systems
- Scalability in agent-based simulation

STEERING COMMITTEE

- **Cossentino, Massimo**, ICAR-CNR, Italy
- **Fortino, Giancarlo**, Universita della Calabria, Italy
- **Gleizes, Marie-Pierre**, Universite Paul Sabatier, France
- **Pavon, Juan**, Universidad Complutense de Madrid, Spain
- **Russo, Wilma**, Universita della Calabria, Italy

SECTION EDITORS

- **Fuentes-Fernández, Rubén**, Research Group on Agent-based, Social & Interdisciplinary Applications (GRASIA), University Complutense of Madrid (UCM), Spain
- **Gravina, Raffaele**, University of Calabria, Italy
- **Niazi, Muaz**, COSMOSE Research Group, COMSATS Institute of IT, Pakistan
- **Seidita, Valeria**, Università degli Studi di Palermo, Italy

REVIEWERS

- **Antunes, Luis**
- **Azar, Ahmad Taher**, Benha University, Egypt, Egypt
- **Bernon, Carole**, Universite Paul Sabatier, France
- **Bremer, Joerg**, University of Oldenburg
- **Cipresso, Pietro**, Applied Technology for Neuro-Psychology Lab, Italy
- **Davidsson, Paul**, Malmö University, Sweden
- **Derksen, Christian**, University Duisburg-Essen, Germany
- **Fortino, Giancarlo**, Universita della Calabria, Italy
- **Garro, Alfredo**, University of Calabria, Italy
- **Guerrieri, Antonio**, University of Calabria, Italy
- **Kowalczyk, Ryszard**, Swinburne University of Technology, Melbourne, Victoria, Australia
- **Linnenberg, Tobias**
- **Moench, Lars**, FernUniversität Hagen, Germany
- **Molesini, Ambra**, Università di Bologna, Italy
- **Özdemir, Serkan**, University of Duisburg-Essen, Germany
- **Petta, Paolo**, OFAI, Austria
- **Ribino, Patrizia**, Istituto di Reti e Calcolo ad Alte Prestazioni - Consiglio Nazionale delle Ricerche, Italy
- **Savaglio, Claudio**, Universita della Calabria
- **Sonnenschein, Michael**, University of Oldenburg, Germany
- **Sudeikat, Jan**, Hamburg Energie GmbH, Germany
- **Törsleff, Sebastian**
- **Unland, Rainer**, Universität Duisburg-Essen, Germany
- **Vizzari, Giuseppe**, Università di Milano Bicocca, Italy
- **Zia, Kashif**, Sohar University, Oman, Pakistan

On local minima in distributed energy scheduling

Astrid Nieße*, Jörg Bremer†, Sebastian Lehnhoff†

*R&D Division Energy, OFFIS – Institute for Information Technology, Escherweg 2, D-26121 Oldenburg, Germany
Email: {astrid.niesse}@offis.de

†Energy Informatics, Department of Computing Science, University of Oldenburg, D-26111 Oldenburg, Germany
Email: {joerg.bremer, sebastian.lehnhoff}@uni-oldenburg.de

Abstract—Distributed energy scheduling constitutes a tough task for optimization algorithms, as the underlying problem structure is highdimensional, multimodal and non-linear. For this reason, metaheuristics and especially distributed algorithms have been in the focus of research for several years with promising results. The modeling of the distributed energy units' flexibility is a specific research task, with different concepts like comfort-level based approaches, enumeration of possible schedules, and continuous schedule representation using machine learning and decoder techniques. Although a continuous representation of flexibility has shown better results regarding the global optimization goal, there have been hints that the susceptibility to local minima traps enlarges compared to the enumeration of distinct schedules. In this contribution, we present an exemplary system for predictive scheduling of distributed energy units consisting of a continuous flexibility modelling approach and a fully distributed planning heuristic. A prestudy is presented, where we analyze the problem structure regarding local minima and describe planned work to reduce the heuristic's susceptibility to be kept in these.

Index Terms—Distributed Energy Scheduling, Agent-Based Control, Self-Organization, Unit Commitment, Local Minima, Meta-Heuristics.

I. INTRODUCTION

IN FUTURE energy systems, distributed energy units like renewables, small combined heat and power (CHP) plants, and electrical storages are needed for both energy provision and grid stabilization purposes. Typically, these units are operated in an aggregated fashion by so-called virtual power plants (VPP), constituting the core concept for renewable energy systems [1]. One of the main challenges during operation of such a VPP arises from the complexity of the scheduling task due to the large amount and the diverse nature of energy units in the distribution grid [2].

The general optimization problem to be solved for this scheduling task is known as unit commitment problem [3] and constitutes a combinatorial optimization problem: Under given constraints specific for the respective energy units (local constraints) operation modes for each unit have to be chosen in such a way that the global optimization goal is reflected for the whole planning horizon. These kind of problems have been described as multiple-choice subset-sum problem [4]. It has been shown that for the given task of predictive scheduling the problem is weakly NP-complete, if the continuous operation of

energy units is discretized to operation states per time interval (schedules) [5]. Following this discretization, the optimality depends on the combination of the schedules of all energy units in each interval.

Thus, the problem of predictive scheduling in VPP shows the following characteristics: First, for day-ahead scheduling with a resolution of 96 time intervals the problem is high-dimensional. Second, the combinations of schedules may show the same performance with different combinations of schedules – thus the problem is multimodal. Third, with the non-convex structure of the solution space that is given with the physical properties of the energy units, the problem has to be classified as non-linear. Due to this structure of the optimization problem, several heuristic optimization algorithms have been proposed and evaluated for predictive scheduling in VPP [5], [6], [7], [8].

With the concept of schedules as discretized operation modes, a reduced view on the potential flexibility of the respective energy unit is chosen: While some units may be operated in a fine-grained manner, the coarse grained solution space narrows schedule choices to a distinct set of schedules without tapping the units' full optimization potential. To this end, a support vector data description (SVDD) model and a decoder approach have been introduced [9], allowing for a continuous representation of flexibility combined with a targeted unconstrained search based on this surrogate model. Although the usage of the decoder largely helps to identify solutions that better use the units' flexibility [10], there has been evidence that the amount of local minima increases as well. With the general predisposition of heuristic algorithms to local minima [11] a more in-depth analysis of the relation of flexibility modelling and optimization performance is necessary: The combination of a search space representation and the heuristic using this search space has to be chosen carefully [12].

In this contribution we present a preliminary study on the predisposition of the combination of SVDD based flexibility modelling, decoder based search and the distributed optimization heuristic COHDA [5] for local minima and give an outline of planned work to analyze the dependencies in greater depth.

The rest of this position paper is structured as follows: In section II we give an introduction to different approaches to flexibility modelling, followed by an overview on distributed energy scheduling in section III. We then present a preliminary study on the occurrence of local minima in different search space settings and conclude with an outline of planned work.

Parts of this work have been funded by the Lower Saxony Ministry of Science and Culture through the 'Niedersächsisches Vorab' grant programme (grant ZN3043) within the research project 'NEDS – Nachhaltige Energieversorgung Niedersachsen'.

II. FLEXIBILITY MODELING

Flexibility modeling can be understood as the task of modeling constraints for energy units. Apart from global VPP constraints, constraints often appear within single energy components; affecting the local decision making. Popular methods treat constraints or aggregations of constraints as separate objectives or penalties, leading to a transformation into a (unconstrained) many-objective problem [13], [11].

For optimization approaches in smart grid scenarios, black-box models capable of abstracting from the intrinsic model have proved useful [14], [15]. The units do not need to be known at compile time. A powerful, yet flexible way of constraint-handling is the use of a decoder that gives a search algorithm hints on where to look for schedules satisfying local hard constraints [15], [16].

A decoder is a technique that gives algorithms hints on where to look for feasible solutions and thus allows for a targeted search. It imposes a relationship between a decoder solution and a feasible solution and gives instructions on how to construct a feasible solution [16]. Using directly a given set \mathcal{X} of feasible schedules derived from a simulation model can already serve as a decoder [5] without a need for machine learning techniques to deduce a meta-model, a response surface, or similar. Each schedule is simply mapped on the most similar one from \mathcal{X} with the lowest distance.

We regard a schedule of an energy unit as a vector $\mathbf{x} = (x_0, \dots, x_d) \in \mathcal{F} \subset \mathbb{R}^d$ with each element x_i denoting mean power generated (or consumed) during the i th time interval.

A simple, yet easy way to find a surrogate model for the flexibility of an energy unit is to abstract from operation and constraints by maintaining a set \mathcal{S} of feasible example schedules and use this set as abstraction layer. Any given schedule \mathbf{x} is feasible iff $\mathbf{x} \in \mathcal{S}$. A relaxed variant might demand that $\exists \hat{\mathbf{x}} \in \mathcal{S} \bullet \|\hat{\mathbf{x}} - \mathbf{x}\| \leq \epsilon$ for some small, given threshold. We take the strict version.

So far, this surrogate is capable of checking feasibility when already given a schedule. In this way, the surrogate may tell apart feasible and infeasible schedules on behalf of the specific simulation model of the energy unit and thus already allows for an abstraction from any model specific implementation. On the other hand, it is not yet a sufficient constraint-handling technique as it still needs externally (e. g. by any optimization algorithm) generated schedules which can merely be checked. Hence, we need to guide an algorithm where to look for feasible schedules. A decoder can do this. For the set based approach, a decoder can simply be derived as follows:

$$\tau_{\text{set}} : \begin{cases} \mathbb{R}^d \rightarrow \mathcal{S} \\ \mathbf{x} \mapsto \mathbf{x}' \in \mathcal{S}, \|\mathbf{x} - \mathbf{x}'\| < \|\mathbf{x} - \mathbf{x}^*\| \quad \forall \mathbf{x}^* \in \mathcal{S}, \mathbf{x}' \neq \mathbf{x}^* \end{cases} \quad (1)$$

In this way, any given (feasible or not) schedule \mathbf{x} is mapped onto the nearest feasible schedule from \mathcal{S} . The granularity of this model depends on the cardinality of the set \mathcal{S} . The larger $|\mathcal{S}|$ the more the model resembles a continuously modeled feasible space. We will now discuss a way of modeling flexibility in a real continuous space.

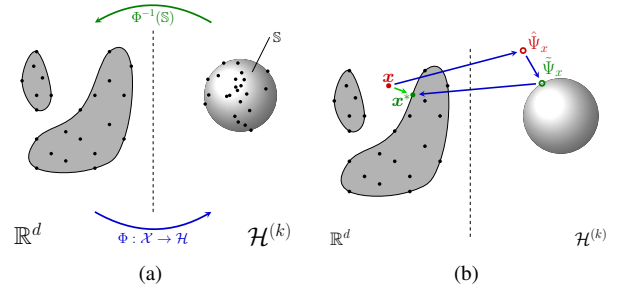


Fig. 1. General support vector decoder scheme for solution repair and constraint handling [19].

Fig. 1 shows the idea of a support vector decoder starting with a set of feasible example schedules derived from a simulation model of the respective energy unit and using it as a stencil for the region that contains just feasible schedules.

A training set \mathcal{X} containing only valid schedules, can e. g. be derived after a sampling approach from [17]. From such training set, a SVDD [18] derives a geometrical description of the sub-space that contains the given data (in our case: the set of feasible schedules). Given a set of data samples, the enclosing envelope can be derived as follows: After mapping the data to a high dimensional feature space, the smallest enclosing ball in this feature space is determined. When mapping back the ball to data space, it forms a set of contours enclosing the given data sample.

This task is achieved by determining a mapping $\Phi : \mathcal{X} \subset \mathcal{F} \subset \mathbb{R}^d \rightarrow \mathcal{H}; \mathbf{x} \mapsto \Phi(\mathbf{x})$ such that all data from a sample \mathcal{X} is mapped to a minimal hypersphere in \mathcal{H} . The minimal sphere with radius R and center a in \mathcal{H} that encloses $\{\Phi(\mathbf{x}_i)\}_N$ can be derived from minimizing $\|\Phi(\mathbf{x}_i) - a\|^2 \leq R^2 + \xi_i$ with slack variables $\xi_i \geq 0$ for a smoother ball.

After some relaxations one gets two main outcomes: the center $a = \sum_i \beta_i \Phi(\mathbf{x}_i)$ (with β weighting the impact of different schedules) of the minimal sphere in terms of an expansion into \mathcal{H} and a function that allows to determine the distance of the image of an arbitrary point from $a \in \mathcal{H}$, calculated in \mathbb{R}^d is derived: $R^2(\mathbf{x}) = 1 - 2 \sum_i \beta_i k_G(\mathbf{x}_i, \mathbf{x}) + \sum_{i,j} \beta_i \beta_j k_G(\mathbf{x}_i, \mathbf{x}_j)$. Because all support vectors are mapped onto the surface of the sphere, the sphere radius R_S can be easily determined by the distance of an arbitrary support vector to the center a . Thus the feasible region can now be modeled as $\mathcal{F} = \{\mathbf{x} \in \mathbb{R}^d | R(\mathbf{x}) \leq R_S\} \approx \mathcal{X}$.

The model can be used as a black-box that abstracts from any explicitly given form of constraints and allows for a decision on whether a given solution is feasible or not. From the support vector model, a decoder can be derived automatically. The set of feasible schedules is represented as pre-image of a high-dimensional ball \mathcal{S} . Fig. 1(a) shows the geometric situation. This representation has some advantageous properties. Although the pre-image might be some arbitrary shaped non-continuous blob in \mathbb{R}^d , the high-dimensional representation is a ball and thus geometrically easier to handle.

If a schedule is feasible it is inside the feasible region (grey area on the left in Fig. 1(b)). Thus, the schedule is

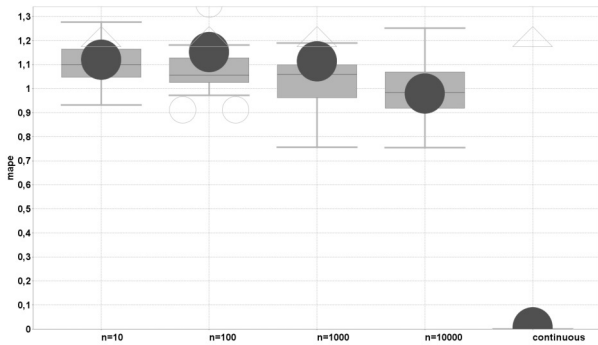


Fig. 2. Solution quality (as mean absolute percentage error, mape) as a function of the granularity of the flexibility model.

inside the pre-image (representing the feasible region) of the ball and thus its high-dimensional image lies inside the ball. An infeasible schedule (e.g. \mathbf{x} in Fig. 1(b)) lies outside the feasible region and thus its image $\hat{\Psi}_x$ lies outside the ball. But we know some relations: the center of the ball, the distance of the image from the center and the radius of the ball. Hence, we can move the image of an infeasible schedule along the difference vector towards the center until it touches the ball. Finally, one can calculate the pre-image of the moved image $\tilde{\Psi}_x$ and get a schedule at the boundary of the feasible region: a repaired schedule \mathbf{x}^* that is now feasible. No mathematical description of the original feasible region or of the constraints is needed to do this. More sophisticated variants of transformation are e.g. given in [9]. Formally, the decoder τ is given by

$$\tau : \mathbb{R}^d \rightarrow \mathcal{F}_{U_i} \subseteq \mathbb{R}^d, \mathbf{x} \mapsto \tau(\mathbf{x}) = \hat{\Phi}^{-1} \circ \tau_{\text{move}} \circ \hat{\Phi}. \quad (2)$$

Using any decoder, the global scheduling problem can be transformed into a formulation that is unconstrained regarding local constraints. Apart from finding a combination of schedules whose sum resembles a given target power profile best, further objectives are usually integrated due to the many-objective nature of energy scheduling. In the following, we consider predictive scheduling, where the goal is to select exactly one schedule \mathbf{x}_i for each energy unit U_i from a search space of feasible schedules with respect to a future planning horizon, such that a global objective (e.g. resembling a target power profile) is optimized by the sum of individual contributions [10]. A basic formulation of the scheduling problem is given by

$$\delta \left(\sum_{i=1}^m \mathbf{x}_i, \zeta \right) \rightarrow \min; \text{ s.t. } \mathbf{x}_i \in \mathcal{F}^{(U_i)} \forall U_i \in \mathcal{U}. \quad (3)$$

In equation (3) δ denotes a distance measure for evaluating the difference between the aggregated schedule of the VPP and the desired target schedule ζ . To compare results and for scalability reasons we used the mean absolute percentage error (mape) $\delta(\mathbf{x}, \zeta) = \frac{100}{d} \sum_{i=1}^d \left| \frac{\zeta_i - x_i}{\zeta_i} \right|$.

To each energy unit U_i exactly one schedule \mathbf{x}_i has to be assigned. $\mathcal{F}^{(U_i)}$ denotes the individual set of feasible schedules

that are operable for unit U_i without violating any (technical) constraint. Solving this problem without unit independent constraint handling leads to specific implementations that are not suitable for handling changes in VPP composition or unit setup without having changes in the implementation of the scheduling algorithm [15]. Using a decoder for constraint handling one can now rephrase the optimization problem as

$$\delta \left(\sum_{i=1}^m \tau_i(\mathbf{x}_i), \zeta \right) \rightarrow \min, \quad (4)$$

where τ_i is the decoder function of unit i that produces feasible schedules from $\mathbf{x} \in [0, x_{max}]^d$ resulting in schedules that are operable by that unit. Please note, that this is a constraint free formulation. With this problem formulation, many standard algorithms for optimization can be easily adapted as there are no constraints (apart from a simple box constraint $\mathbf{x} \in [0, x_{max}]^d$) to be handled and no domain specific implementation (regarding the energy units and their operation schedules) has to be integrated in the optimization algorithm. Equation (4) is used as a surrogate objective to find the solution to the constrained optimization problem Eq. (3).

Fig. 2 shows some mean optimization results obtained by using different flexibility models. Four discrete flexibility models (cf. decoder Eq. 1) have been used with sets ranging from $n = 10$ to 10000 elements (schedules). Additionally one fully continuous flexibility model has been used. It is obvious that the optimization result gets better the more choices are contained in the model. Moreover, a significant improvement can be made by transition to a fully continuous model. On the other hand, with growing granularity, the variance of the results and the number of worse outliers also grow indicating a growing risk to premature convergence. Also in the continuous case outliers indicating results worse than with the coarse grained model (upper triangle) are present. This result also reproduces preliminary results from [10].

It seems immediately advantageous to use continuous or at least fine grained models to obtain better results. On the other hand, this design decision entails a growing complexity and a larger modality to the objective making the problem harder to solve due to problems with premature convergence. We will show this in greater detail in the following section.

III. DISTRIBUTED ENERGY SCHEDULING

Heuristic and especially distributed and agent-based algorithms have been in the focus of research within the last years. Nevertheless, the notion of what constituted a distributed algorithms still differs a lot: Whereas early publications focussed on the atomic units (mainly named agents) as a gateway to distributed energy units, many hierarchical approaches have been presented for both energy market aspects [20], [21], [22] as balancing approaches [23]. In recent years, some fully distributed algorithms have been presented, with the individual agents being capable of solution generation and evaluation without a centralized components [24], [25].

The Combinatorial Optimization Heuristic for Distributed Agents (COHDA, originally introduced in [5]) has been evaluated for predictive scheduling problems in VPPs and has been chosen for our analysis of local minima susceptance with a continuous flexibility model. Although parts of the planned work regarding local minima convergence reduction is specific for COHDA (the algorithmic parts), the general problem analysis is valid for all heuristic distributed algorithms using a continuous flexibility model. In the following, COHDA is described in a concise fashion, based on the description in [26].

A. Introducing COHDA

The key concept of COHDA is an asynchronous iterative approximate best-response behavior, where each agent – representing a decentralized energy unit – reacts to updated information from other agents by adapting its own selected schedule with respect to the global objective function (OF). All agents $a_i \in A$ initially only know their own respective set of schedules S_i . From an algorithmic point of view, the difficulty of the problem is given by the distributed nature of the system in contrast to the task of finding a common allocation of schedules for a global target power profile.

Thus, the agents coordinate by updating and exchanging information about each other. For privacy and communication overhead reasons, the potential flexibility (i.e. the set of feasible schedules) S_i is not communicated as a whole by an agent a_i . Instead, the agents communicate single selected schedules within the approach as described in the following.

First of all, the agents are placed in an artificial communication topology based on the small-world scheme, such that each agent is connected to a non-empty subset of other agents. This overlay topology might be a ring in the least connected variant.

Each agent a_i collects two distinct sets of information: on the one hand the believed current configuration γ_i of the system (that is, the most up to date information a_i has about currently selected schedules of all agents), and on the other hand the best known combination γ_i^* of schedules with respect to the global objective function it has encountered so far.

Beginning with an arbitrarily chosen agent by passing it a message containing only the global objective (i.e. the target power profile), each agent repeatedly executes the three steps *perceive*, *decide*, *act* (cf. [26]) as visualized in Fig. 3:

- 1) **perceive:** When an agent a_i receives a message κ_p from one of its neighbors (say, a_p), it imports the contents of this message into its own memory.
- 2) **decide:** The agent then searches S_i for the best schedule regarding the updated system state γ_i and the global objective function. Local constraints are taken into account in advance. Details regarding this procedure have been presented in [19]. If a schedule can be found that satisfies both the objectives, a new schedule selection is created. If the resulting modified system state γ_i yields a better rating than the current solution candidate γ_i^* , a new solution candidate is created based on γ_i . Otherwise

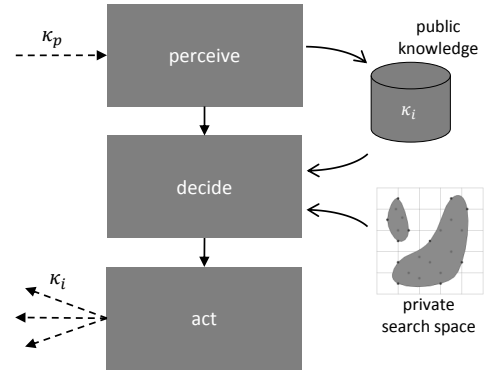


Fig. 3. The *perceive–decide–act* behavioral pattern in COHDA from the point of view of an agent a_i [19].

the old solution candidate still reflects the best schedule combination regarding the global objective the agent is aware of, so the just created schedule selection is discarded and the agent reverts to its schedule selection stored in γ_i^* .

- 3) **act:** If γ_i or γ_i^* has been modified in one of the previous steps, the agent finally broadcasts these to its neighbors in the communication topology.

Following this behavior, only small subsets of the sets of feasible schedules S_i are communicated by the agents. During this process, for each agent a_i , its observed system configuration γ_i as well as solution candidate γ_i^* are filled successively. After producing some intermediate solutions, the heuristic eventually terminates in a state where for all agents γ_i as well as γ_i^* are identical, and no more messages are produced by the agents. At this point, γ_i^* is the final solution of the heuristic and contains exactly one schedule selection for each agent.

B. Convergence of COHDA in local minima

During the above described phases *perceive*, *decide*, and *act*, a better solution candidate always prevails over inferior solution candidates, and the system always terminates with convergence. Due to the asynchronous search in the solution space, inferior local optima are discarded as long as other agents are able to identify better solutions.

The susceptibility to local minima convergence depends on both the structure of the solution space and the search algorithm. With a course-grained representation of schedules as enumerated set, COHDA always reached near-optimal convergence [5]. In the following we present results of two application examples of COHDA where this behavior can not be guaranteed and thus motivate a deeper analysis of local minima susceptibility.

1) *Continuous scheduling:* In [19], COHDA has been coupled with a continuous flexibility modeling approach, thus allowing for a targeted search within that search space and delivering a fine-grained flexibility description. This system has been applied for the task of continuous scheduling in VPP: after an initial predictive scheduling, incidents (DER

breakdowns, prognoses faults, ...) may render the initial schedules infeasible. In this case, the infeasible schedules have been marked as invalid and an adapted variant of COHDA has been restarted for a new cooperative search.

In Fig. 4 an exemplary outcome of such a continuous scheduling process with 10 CHP outages is shown. On the x-axis, the solution evaluation is chronologically ordered: Each time an agent evaluates a VPP schedule within the OF, this is logged within the system. On the y-axis, the expected product delivery performance is given. A value of 1.0 means perfect product delivery (i.e. 150 kWh in all 4 product hours). In the left part of the diagram, the initial planning process is shown: The agents yield an expected product delivery performance of 0.99 in the day ahead planning process. For all following values, the simulated time is given on top of the diagram for ease of understanding. Incidents are depicted using arrows.

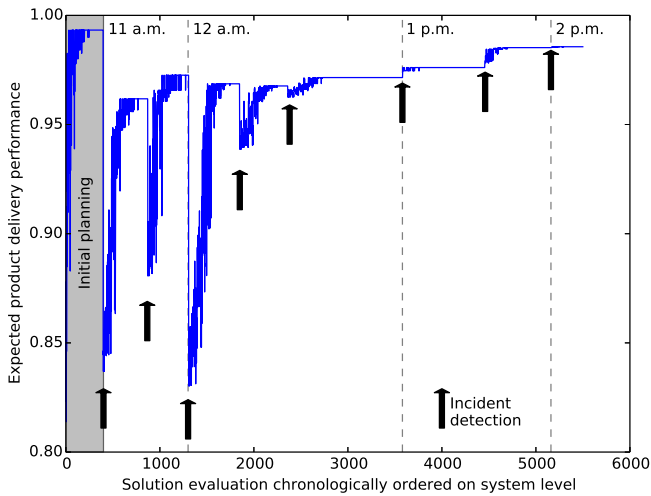


Fig. 4. Example for incident detection and expected product delivery performance [27].

In the first half of product delivery, each incident leads to an initially reduced product delivery performance. The agents manage to enhance this value within the cooperative search for a new VPP schedule though. Convergence of the processes can be recognized from the plateaus before the next incident.

During the second half of product delivery, an effect not yet explained is observed: with an incident, the product delivery performance does not decrease as expected, but increases to a better value at once. A possible explanation for this might be that the incidents lead to a restart of the heuristic and thus an escape from a local minimum. In Fig. 4 only one exemplary optimization restart process is given. During the examination of the approach presented in [27] the effect of a better performance after disturbance has been observed several times, even with the effect of a better performance after an incident compared to the initial predictive scheduling.

2) *Reducing evaluation sensitivity:* Due to the continuous representation of the flexibility, it is not possible to calculate the global optimum even in small scenarios. Therefore, the analysis if a simulation has converged within a local minimum cannot be done using a brute force approach in the combined system of COHDA and SVDD based flexibility description. To analyze the suspection to local minima of this combined system, a trick can be chosen: In spite of analysing the problem structure, the sensitivity of the agents when analysing the problem structure and searching for a new solution candidate can be changed by artificially reducing the precision within the OF.

In Fig. 5, results of this approach are shown for a scenario with 100 energy units (CHP and PV plants). The agents had to plan a product of 600 kWh to be delivered within one hour. The results for product fulfillment (with a value of 1.0 denoting perfect fulfillment of 600 kWh and values above 1.0 denoting overfulfillment), simulation duration until convergence and cooperation overhead (total amount of messages until convergence). For all settings of the sensitivity value, the problem structure has been the same. The precision of the optimization evaluation has been modified from 0.0 (i.e. full precision) to 0.01. It can be seen that with a larger sensitivity value, both simulation duration and cooperation overhead go down. The result quality though, given as product fulfillment, seems to be instable: While with a sensitivity value of 0.005 all simulation runs lead to a product fulfillment close to 1.0, the opposite is the case with a value of 0.01: All simulation runs converge with a product fulfillment of 1.2, a local minimum that already has been encountered in the other runs. Obviously, the system has been trapped in a local minimum in the last simulation series.

Up to now, we did not analyze the effects of combining the continuous flexibility representation with COHDA in sufficient detail. With these results, it has been decided to analyze the context of continuous flexibility modeling, COHDA and local minima susceptibility on more detail.

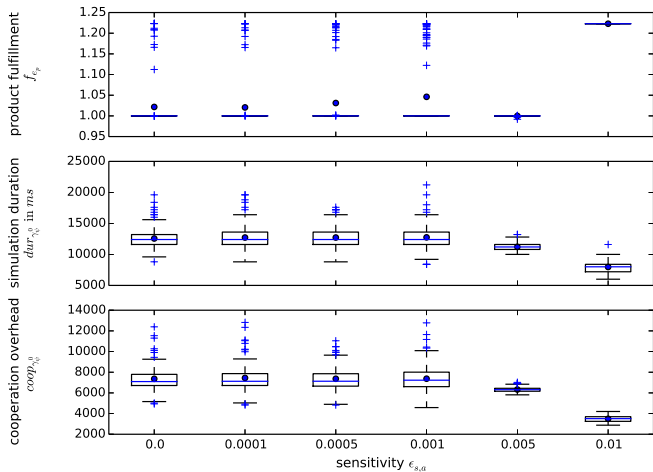


Fig. 5. Product fulfillment, simulation duration and cooperation overhead with rising sensitivity values, adapted from [28]. Each simulation set shows the result of 100 simulation runs as boxplot.

IV. PRESTUDY: OCCURENCE OF LOCAL MINIMA

In order to underpin our conjectures regarding the increase of local minima with introducing fine grained flexibility modeling, we investigated the changes in problem complexity with means from fitness landscape analysis.

A. Structure analysis

We start by analyzing the structure of fitness landscapes. A landscape \mathcal{L} is defined by the search space \mathcal{S} , a neighborhood relation \mathcal{N} and an error function (equivalently: the fitness) ν . Plotting ν over all $x \in \mathcal{S}$ yields the landscape that is scanned by some optimization algorithm for the optimal point. The structure of this landscape determines (premature) convergence and thus whether the algorithm succeeds with a sufficiently small budget or gets stuck within some local optimum.

One can analyze the structure of this landscape e. g. by scrutinizing the error correlation of neighboring candidate solutions [29]. Neighboring solutions from flat regions of the landscape exhibit a higher correlation than solutions from rugged parts of the landscape. Thus, the correlation can be seen as some measure for the ruggedness of \mathcal{L} .

We scrutinize the autocorrelation of random paths on the landscape (random walk through \mathcal{N}) [30]. Let $X = (x_{ij})$ be a solution of the predictive scheduling problem Eq. (4) with each row denoting a schedule for unit i and each element representing mean active power during the respective time interval j . Let $\{f_t\}_{t=1}^n$ be a sequence of n objective values, sampled as follows: starting from a randomly chosen solution $X_1 \in \mathcal{S}$ successive, neighboring solutions X_{t+1} are generated after [31] by altering each element in X_t by adding or subtracting 0.1 with a probability of 1/3 each. It is ensured that the solution stays within the feasible region and that at least one element of X_t is altered. The series $F = \{f_t\}_{t=1}^n$ now contains values $f_t = \nu(X_t)$, with $\nu(X) = \delta(\sum_{x_i \in X} x, z)$.

Now one can calculate the autocorrelation

$$\rho(\sigma) = \frac{E[f_t f_{t+\sigma}] - E[f_t]E[f_{t+\sigma}]}{V[f_t]} \quad (5)$$

for a given path length σ , with $E[f_t]$ and $V[f_t]$ denoting expectation and variance respectively. Moreover, [30] defines the correlation length $\lambda = -\frac{1}{\ln(\rho(1))}$, denoting the mean distance (in the sense of neighboring hops of \mathcal{N}) from which the majority of the solutions is no longer correlated [29]. The correlation length can also be interpreted as the expected maximum width of flat valleys in the landscape.

B. Information analysis

Analyzing the correlation of random paths on the landscape yields an impression of the structure. In [29] an extended analysis is proposed based on entropy measures on $\{f_t\}_{t=1}^n$. Founded on ideas from algorithmic information theory [32] and the entropy from Shannon [33], a characterization of the distribution and number of local optima along the path is given as a measure of the complexity of the fitness landscape.

For the following indicators, random paths on the landscape are seen as ensemble of base elements. Three element types

(token) can be distinguished: flat areas (neighboring points have similar fitness), isolated points (surrounded merely by better, or worse points), and slope points (neither isolated nor flat). In a first step, each path is transformed in a sequence of tokens $S(\epsilon) = s_1 s_2 \dots s_n$ over the alphabet $\{\bar{1}, 0, 1\}$ by

$$S_i = \psi_{f_t}(i, \epsilon) = \begin{cases} \bar{1}, & \text{if } f_i - f_{i-1} < -\epsilon \\ 0, & \text{if } |f_i - f_{i-1}| \leq \epsilon \\ 1, & \text{if } f_i - f_{i-1} > \epsilon \end{cases} \quad (6)$$

for a given $\epsilon \in [0, \max f_i]$ (cf. [29]) A string $S(\epsilon)$ then contains information on the structure of the landscape along a randomly chosen path. Now one can define an object by two successive tokens in the string. For example, the sequence $\bar{1}1$ denotes a change from downslope to upslope and thus a trough. The entropy measure for such an ensemble of objects can be determined after [29]:

$$H(\epsilon) = - \sum_{p \neq q} P_{[pq]} \log_6 P_{[pq]}, \quad (7)$$

with $P_{[pq]}$ denoting the frequency of the occurrence of the sequence pq in $S(\epsilon)$. The modality of the objective function can also be derived from $S(\epsilon)$. As opposed to the entropy which is a measure of the diversity of objects along the path, the modality must be measured by a classification of objects in order to determine the number of (local) optima. First, the partial information content is determined [29]. To achieve this, the string $S(\epsilon)$ is transformed into $S'(\epsilon) = o_1 o_2 \dots o_\mu$ over the alphabet $\{\bar{1}, 1\}$. This yields the shortest string that represents the alternations from uphill to downhill changes along the path. The partial information content is recursively defined by [29]:

$$M(\epsilon) = \frac{\mu}{n} = \frac{|S'(\epsilon)|}{|S(\epsilon)|} \in [0, 1]. \quad (8)$$

A value of 1 denotes the maximum modality. The absolute number of (local) optima (according to a given ϵ) can be derived by $\lfloor (n \cdot M(\epsilon))^{-2} \rfloor$. All these measures are sensitive to the choice of ϵ . Small values lead to a higher sensitivity to changes in fitness between neighbouring solution. The smallest value of ϵ that lets all differences vanish is called information stability [29] (fully flat error function).

C. Results

As a unit model we used a co-generation model that has already served in several studies and projects for evaluation [34], [35], [10], [36]. This model comprises a micro CHP bundled with a thermal buffer store. Constraints restrict power band, buffer charging, gradients, min. on and off times, and satisfaction of thermal demand. Thermal demand is determined by simulating a detached house. For each agent the model is individually (randomly) configured with state of charge, weather condition, temperature range, allowed operation gradients, and similar. We experimented with problem sizes of 20 energy units for scheduling.

First, we scrutinized the complexity of the fitness landscape using the correlation analysis. Figure 6(a) shows the result.

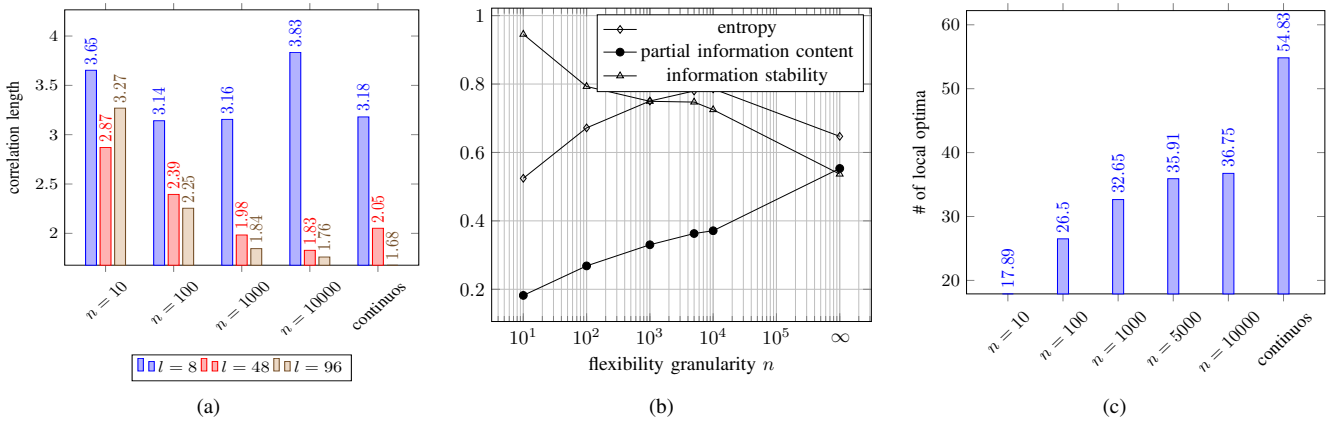


Fig. 6. Experimental results of the fitness landscape analysis.

 TABLE I
 COMPARISON OF DIFFERENT TYPES OF ENERGY UNITS.

unit type	entropy	part. inf.	# local optima	inf. stability
heat pump	0.708 ± 0.045	0.495 ± 0.039	49.04 ± 3.91	0.462 ± 0.095
boiler	0.69 ± 0.046	0.459 ± 0.039	45.48 ± 3.93	0.372 ± 0.171
cool storage	0.501 ± 0.096	0.171 ± 0.050	16.74 ± 5.03	0.709 ± 0.173
chp	0.354 ± 0.097	0.113 ± 0.044	11.13 ± 4.42	0.943 ± 0.104

Comparing the correlation length of the scheduling problem with different granularity of flexibility modeling, one can derive that the complexity grows with finer grained models. The correlation length almost vanishes with the continuous model. Thus, neighboring solutions are mostly uncorrelated with fine grained models. This result is immediately apparent as the coarse grained models map many neighboring solutions onto the very same phenotype solution, resulting in a higher correlation. The experiment has been conducted for different schedule lengths. The effect is different for different problem complexities (cf. Fig. 6(a)), because shorter schedules exhibit less regions with high information content [15].

Fig. 6(b) shows results of the information analysis. Whereas information stability and partial information indicate a rising modality with rising granularity in flexibility modeling, the entropy slightly recedes for the continuous case. This might be founded in vanishing steps that are prominent in the discrete case. The result in Fig. 6(c) most prominently shows the difference in complexity when comparing the discrete and the continuous flexibility models: the mean (absolute) number of local minima that are encountered along a random path across the fitness landscape. Although the absolute number depends on path length (200 in this case) and on the choice of ϵ , the general trend is still always the same for this experiment.

Obviously, also the types of modeled energy units have an impact on these results. Table I compares the results for different problems with different types of energy units.

V. CONCLUSION AND FURTHER WORK

Predictive scheduling with its combinatorial optimization problem is a frequent task in future virtual power plants. As

any algorithm implementation should be designed independently from the aggregated energy units an abstraction layer renders indispensable. Flexibility modeling with decoders allows integrating any energy unit into the optimization model without domain specific knowledge on the possible future operations, technical constraints or on the structure of the individual search space of feasible schedules by building up a constraint-free search space.

Flexibility modeling may be achieved with different surrogate techniques. First we presented hints from earlier studies to problems regarding local minima susceptance with a fine-grained decoder based flexibility model. Then we scrutinized the effect of two possible implementations and showed the dependencies on the granularity of the model: Fine grained or continuous models allow for higher precision and better optimization results and are thus desirable. On the other hand, such fine grained models introduce complexity by additional local minima in the objective.

These results lead up to further work, with the general goal of (a) getting a deeper understanding of the predisposition of fine-grained flexibility modeling combined with distributed algorithms for predictive scheduling to premature local minima convergence and (b) analyzing algorithmic adaptations to COHDA to reduce premature local minima convergence rates. The following studies will be conducted with these goals:

- 1) Topology adaptations: For COHDA, different overlay topologies have been analyzed in detail. After a first setup of the agents' neighborhood though, no adaptations have been made during an ongoing optimization. In a simulation study we want to analyze the effect of dynamically adapting the communication topology on local minima convergence.
- 2) Artificial restart: There have been indications that the result quality benefits from a restart of the cooperative search within COHDA (see figure 4). To fully understand this effect, we plan to artificially restart an already terminated optimization (e. g. by schedule invalidation, minor target adaptation, or similar).
- 3) Sensitivity adaptations: In preliminary studies we could

show that introducing a sensitivity factor to the OF leads to changes within the local minima convergence. In these studies though, the factor has been chosen statically. In future work, we plan to dynamically adapt this factor, using approaches like simulated annealing.

Later work could include a change in the reaction delay of the agents and a temporary acceptance of deprecated solutions. For the latter, the convergence has to be assured.

REFERENCES

- [1] H.-J. Appelrath, H. Kagermann, and C. Mayer, Eds., *Future Energy Grid. (acatech STUDY)*. acatech, Munich, 2012.
- [2] S. McArthur, E. Davidson, V. Catterson, A. Dimeas, N. Hatziaargyriou, F. Ponci, and T. Funabashi, "Multi-agent systems for power engineering applications – Part I: Concepts, approaches, and technical challenges," *IEEE Transactions on Power Systems*, vol. 22, no. 4, pp. 1743–1752, 2007. doi: 10.1109/TPWRS.2007.908471
- [3] N. Padhy, "Unit Commitment - A Bibliographical Survey," *IEEE Transactions on Power Systems*, vol. 19, no. 2, pp. 1196–1205, May 2004. doi: 10.1109/TPWRS.2003.821611
- [4] D. Pisinger, "A minimal algorithm for the multiple-choice knapsack problem," *European Journal of Operational Research*, vol. 83, pp. 394–410, 1994.
- [5] C. Hinrichs, S. Lehnhoff, and M. Sonnenschein, "A Decentralized Heuristic for Multiple-Choice Combinatorial Optimization Problems," in *Operations Research Proceedings 2012*. Springer, 2014. doi: 10.1007/978-3-319-00795-3_43. ISBN 978-3-319-00795-3 pp. 297–302.
- [6] A. Feliachi and R. Belkacemi, "Intelligent Multi-agent system for Smart Grid Power Management," in *Smart Power Grids 2011*, A. Keyhani and M. Marwali, Eds. Springer, 2012, pp. 515–542.
- [7] P. Vrba, V. Mařík, P. Siano, P. Leitão, G. Zhabelova, V. Vyatkin, and T. Strasser, "A Review of Agent and Service-Oriented Concepts Applied to Intelligent Energy Systems," *IEEE Transactions of Industrial Informatics*, vol. 10, no. 3, pp. 1890–1903, 2014.
- [8] G. Anders, F. Siefert, and W. Reif, "A System of Systems Approach to the Evolutionary Transformation of Power Management Systems," in *43. Jahrestagung der Gesellschaft für Informatik e.V. (GI), Informatik angepasst an Mensch, Organisation und Umwelt*. Koblenz: Gesellschaft für Informatik, Köllen Druck+Verlag, 2013.
- [9] J. Bremer and M. Sonnenschein, "Constraint-handling for optimization with support vector surrogate models – a novel decoder approach," in *Proceedings of the 5th International Conference on Agents and Artificial Intelligence (ICAART)*, J. Filipe and A. Fred, Eds., vol. 2. Barcelona, Spain: SciTePress, 2013. doi: 10.5220/0004241100910100 pp. 91–105.
- [10] C. Hinrichs, J. Bremer, and M. Sonnenschein, "Distributed Hybrid Constraint Handling in Large Scale Virtual Power Plants," in *IEEE PES Conference on Innovative Smart Grid Technologies Europe (ISGT Europe 2013)*. IEEE Power & Energy Society, 2013.
- [11] A. Smith and D. Coit, *Handbook of Evolutionary Computation*. Department of Industrial Engineering, University of Pittsburgh, USA: Oxford University Press and IOP Publishing, 1997, ch. Penalty Functions, p. Section C5.2.
- [12] J. Brownlee, *Clever Algorithms*, 1st ed. LuLu, 2011. ISBN 9781446785065
- [13] O. Kramer, "A review of constraint-handling techniques for evolution strategies," *Appl. Comp. Intell. Soft Comput.*, vol. 2010, pp. 1–19, January 2010. doi: 10.1155/2010/185063
- [14] F. Gieseke and O. Kramer, "Towards non-linear constraint estimation for expensive optimization," in *Applications of Evolutionary Computation*, ser. Lecture Notes in Computer Science, A. Esparcia-Alcázar, Ed. Springer Berlin Heidelberg, 2013, vol. 7835, pp. 459–468.
- [15] J. Bremer and M. Sonnenschein, "Model-based integration of constrained search spaces into distributed planning of active power provision," *Comput. Sci. Inf. Syst.*, vol. 10, no. 4, pp. 1823–1854, 2013.
- [16] C. A. Coello Coello, "Theoretical and numerical constraint-handling techniques used with evolutionary algorithms: a survey of the state of the art," *Computer Methods in Applied Mechanics and Engineering*, vol. 191, no. 11–12, pp. 1245–1287, Jan. 2002. doi: 10.1016/S0045-7825(01)00323-1
- [17] J. Bremer and M. Sonnenschein, "Sampling the search space of energy resources for self-organized, agent-based planning of active power provision," in *27th International Conference on Environmental Informatics, EnviroInfo 2013*, B. Page, A. G. Fleischer, J. Göbel, and V. Wohlgenuth, Eds. Hamburg, Germany: Shaker, 2013, pp. 214–222.
- [18] D. M. J. Tax and R. P. W. Duin, "Support vector data description," *Mach. Learn.*, vol. 54, no. 1, pp. 45–66, 2004. doi: http://dx.doi.org/10.1023/B:MACH.000008084.60811.49
- [19] A. Nieße, J. Bremer, C. Hinrichs, and M. Sonnenschein, "Local Soft Constraints in Distributed Energy Scheduling," in *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems (FEDCSIS)*. IEEE, 2016. doi: 10.15439/2016F76 pp. 1517–1525.
- [20] G. Anders, A. Schiendorfer, F. Siefert, J.-P. Steghöfer, and W. Reif, "Cooperative Resource Allocation in Open Systems of Systems," *ACM Transactions on Autonomous and Adaptive Systems*, vol. 10, no. 2, pp. 1–44, 2015. doi: 10.1145/2700323 ACM
- [21] M. Tröschel, *Aktive Einsatzplanung in holonischen Virtuellen Kraftwerken*. Oldenburg: OIWIR, Oldenburger Verl. für Wirtschaft, Informatik und Recht, 2010. ISBN 978-3-939704-55-3
- [22] P. Papadopoulos, N. Jenkins, L. M. Cipcigan, I. Grau, and E. Zabala, "Coordination of the Charging of Electric Vehicles Using a Multi-Agent System," *IEEE Transactions on Smart Grid*, vol. 4, no. 4, pp. 1802–1809, dec 2013. doi: 10.1109/TSG.2013.2274391
- [23] S. Lehnhoff, *Dezentrales vernetztes Energiemanagement - Ein Ansatz auf Basis eines verteilten Realzeit-Multiagentensystems*. Vieweg + Teubner, 2010.
- [24] E. Pournaras, "Multi-level Reconfigurable Self-organization in Overlay Services," Ph.D. dissertation, TU Delft. ISBN 9789461860989 2013.
- [25] B. Schäfer, M. Matthiae, M. Timme, and D. Witthaut, "Decentral Smart Grid Control," *New Journal of Physics*, no. JANUARY, 2015. doi: 10.1088/1367-2630/17/1/015002
- [26] A. Nieße, S. Beer, J. Bremer, C. Hinrichs, O. Lünsdorf, and M. Sonnenschein, "Conjoint Dynamic Aggregation and Scheduling Methods for Dynamic Virtual Power Plants," in *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems*, ser. Annals of Computer Science and Information Systems, M. Ganzha, L. A. Maciaszek, and M. Paprzycki, Eds., vol. 2. IEEE, 2014. doi: 10.15439/2014F76. ISBN 978-83-60810-58-3 pp. 1505–1514.
- [27] A. Nieße and M. Sonnenschein, "A Fully Distributed Continuous Planning Approach for Decentralized Energy Units," in *45. Jahrestagung der Gesellschaft für Informatik e.V. (GI), Informatik, Energie und Umwelt*. Cottbus: Gesellschaft für Informatik, Köllen Druck+Verlag, 2015.
- [28] A. Nieße, "Verteilte kontinuierliche Einsatzplanung in dynamischen virtuellen Kraftwerken," Ph.D. dissertation, Carl von Ossietzky Universität Oldenburg, Oldenburg, 2015.
- [29] V. K. Vassilev, T. C. Fogarty, and J. F. Miller, "Information characteristics and the structure of landscapes," *Evol. Comput.*, vol. 8, no. 1, pp. 31–60, Mar. 2000. doi: 10.1162/106365600568095
- [30] E. Weinberger, "Correlated and uncorrelated fitness landscapes and how to tell the difference," *Biological Cybernetics*, vol. 63, no. 5, pp. 325–336, 1990. doi: 10.1007/BF00202749
- [31] G. Merkurjeva and V. Bolshakovs, "Benchmark fitness landscape analysis," *International Journal of Simulation Systems, Science & Technology (IJSSST)*, vol. 12, no. 2, pp. 38–45, 2011.
- [32] G. J. Chaitin, *Algorithmic information theory*, ser. Cambridge tracts in theoretical computer science. Cambridge, Cambridgeshire, New York: Cambridge University Press, 1987. ISBN 0-521-34306-2
- [33] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, 1948.
- [34] J. Bremer, B. Rapp, and M. Sonnenschein, "Encoding distributed Search Spaces for Virtual Power Plants," in *IEEE Symposium Series in Computational Intelligence 2011 (SSCI 2011)*, Paris, France, 4 2011. doi: 10.1109/CIASG.2011.5953329
- [35] J. Neugebauer, O. Kramer, and M. Sonnenschein, "Classification cascades of overlapping feature ensembles for energy time series data," in *Proceedings of the 3rd International Workshop on Data Analytics for Renewable Energy Integration (DARE'15), ECML/PKDD 2015*. Springer, 2015.
- [36] A. Nieße and M. Sonnenschein, "Using grid related cluster schedule resemblance for energy rescheduling - goals and concepts for rescheduling of clusters in decentralized energy systems," in *SMARTGREENS*, B. Donnellan, J. F. Martins, M. Helfert, and K.-H. Krempels, Eds. SciTePress, 2013. ISBN 978-989-8565-55-6 pp. 22–31.

2nd International Workshop on Language Technologies and Applications

DEVELOPMENT of new technologies and various intelligent systems creates new possibilities for intelligent data processing. Natural Language Processing (NLP) addresses problems of automated understanding, processing and generation of natural human languages. LTA workshop provides a venue for presenting innovative research in NLP related, but not restricted, to: computational and mathematical modeling, analysis and processing of any forms (spoken, handwritten or text) of human language and various applications in decision support systems. The LTA workshop will provide an opportunity for researchers and professionals working in the domain of NLP to discuss present and future challenges as well as potential collaboration for future progress in the field of NLP.

TOPICS

The submitted papers shall cover research and developments in all NLP aspects, such as (however this list is not exhaustive):

- computational intelligence methods applied to language & text processing
- text analysis
- language networks
- text classification
- document clustering
- various forms of text recognition
- machine translation
- intelligent text-to-speech (TTS) and speech-to-text (STT) methods
- authorship identification and verification
- author profiling
- plagiarism detection
- knowledge extraction and retrieval from text and natural language structures
- multi-modal and natural language interfaces
- sentiment analysis
- language-oriented applications and tools
- NLP applications in education
- language networks, resources and corpora

SECTION EDITORS

- **Damaševičius, Robertas**, Kaunas University of Technology, Lithuania
- **Martinčić – Ipšić, Sanda**, University of Rijeka, Croatia
- **Napoli, Christian**, Department of Mathematics and Informatics, University of Catania, Italy
- **Wozniak, Marcin**, Institute of Mathematics, Silesian University of Technology, Poland

REVIEWERS

- **Burdescu, Dumitru Dan**, University of Craiova, Romania
- **Čukić, Bojan**, UNC Charlotte, United States
- **Cuzzocrea, Alfredo**, University of Trieste, Italy
- **Dobrišek, Simon**, University of Ljubljana, Slovenia
- **Gelbukh, Alexander**, Instituto Politécnico Nacional, Mexico
- **Grigonytė, Gintarė**, University of Stockholm, Sweden
- **Harbusch, Karin**, Universität Koblenz-Landau, Germany
- **Kapočiūtė-Dzikiėnė, Jurgita**, Vytautas Magnus University, Lithuania
- **Krilavičius, Tomas**, Vytautas Magnus University, Lithuania
- **Kurasova, Olga**, Vilnius University, Institute of Mathematics and Informatics, Lithuania
- **Maskeliūnas, Rytis**, Kaunas University of Technology, Lithuania
- **Meštrović, Ana**, University of Rijeka, Croatia
- **Mikielić-Preradović, Nives**, University of Zagreb, Croatia
- **Nowicki, Robert**, Czestochowa University of Technology, Poland
- **Poław, Dawid**, Institute of Mathematics, Silesian University of Technology, Poland
- **Pulvirenti, Alfredo**, University of Catania, Italy
- **Rosen, Alexandr**, Charles University, Czech Republic
- **Sanada, Haruko**, Risho University, Japan
- **Skadina, Inguna**, University of Liepaja, Latvia
- **Šnajder, Jan**, University of Zagreb, Croatia
- **Stanković, Ranka**, University of Belgrade, Serbia
- **Starzewski, Janusz**, Czestochowa University of Technology, Poland
- **Steinberger, Josef**, University of West Bohemia, Czech Republic
- **Szymański, Julian**, Gdansk University of Technology, Poland
- **Tahmasebi, Nina**, University of Gothenburg, Sweden
- **Tramontana, Emiliano**, University of Catania, Italy
- **Wang, Lipo**, Nanyang Technological University, Singapore
- **Žabokrtský, Zdeněk**, Charles University

A Web Corpus for eCare: Collection, Lay Annotation and Learning -First Results-

Marina Santini*, Arne Jönsson†*, Mikael Nyström†*

*RISE SICS East, †Linköping University
Linköping, Sweden

marina.santini@ri.se, arne.jonsson@liu.se, mikael.nystrom@liu.se

Marjan Alirezai

Örebro University
Örebro, Sweden

marjan.alirezai@oru.se

Abstract—In this position paper, we put forward two claims: 1) it is possible to design a dynamic and extensible corpus without running the risk of getting into scalability problems; 2) it is possible to devise noise-resistant Language Technology applications without affecting performance. To support our claims, we describe the design, construction and limitations of a very specialized medical web corpus, called *eCare_Sv_01*, and we present two experiments on lay-specialized text classification. *eCare_Sv_01* is a small corpus of web documents written in Swedish. The corpus contains documents about chronic diseases. The sublanguage used in each document has been labelled as "lay" or "specialized" by a lay annotator. The corpus is designed as a flexible text resource, where additional medical documents will be appended over time. Experiments show that the lay-specialized labels assigned by the lay annotator are reliably learned by standard classifiers. More specifically, Experiment 1 shows that scalability is not an issue when increasing the size of the datasets to be learned from 156 up to 801 documents. Experiment 2 shows that lay-specialized labels can be learned regardless of the large amount of disturbing factors, such as machine translated documents or low-quality texts, which are numerous in the corpus.

I. INTRODUCTION

BUILDING a very specialized medical corpus bootstrapped from the web is not a trivial task. The web is indeed a rich textual resource, but it contains many irrelevant or low-quality documents (noisy texts) that may affect the overall usefulness of a corpus. Sorting out noisy documents from the good ones is a tedious, expensive and time-consuming task. Additionally, in the medical field there is often the need to update a document collection with the latest illness-related texts, containing novel findings, new issues or unprecedented cases.

Web corpora are often at the core of Language Technology applications (henceforth LT applications). Since the design and the quality of web corpora affect the reliability and the performance of corpus-based LT applications, we investigate alternative approaches to traditional corpus design and propose an approach that can ensure robustness without affecting the overall performance. In particular, we focus on the relations between performance, scalability and noise on a specific LT task, namely lay-specialized text classification.

Performance can be affected by both scalability issues and by noise. We use the word "performance" to refer to the results achieved on a specific task (e.g. text classification), while with the word "scalability" we refer to the application's ability to adapt to the growing size of the underlying corpus without requiring major design changes. Scalability and performance are often associated, because performance can be affected by scalability issues.

Noise, on the other hand, is pervasive in Language Technology. Normally, LT applications are developed to handle clean texts. These applications may suffer from a significant performance decline when increasing the noise level of the corpus. Cleaning texts or removing noisy documents from a corpus is often a daunting and expensive task. With the expressions "noise resilience" and "noise-resistant LT applications", we refer to the property of keeping up a good performance in the presence of noisy documents.

In this position paper, we argue that: 1) designing dynamic and extensible web corpora does not necessarily imply scalability issues for LT applications; 2) including noisy texts in a corpus does not necessarily imply decreases in performance. Robustness to scalability issues and to noise are desirable qualities of any LT applications.

To support our claims, we describe the design, the construction and the limitations of a very specialized medical web corpus, called *eCare_Sv_01*, and we explore the case of lay-specialized text classification. *eCare_Sv_01* is a small corpus of web documents written in Swedish. The documents in the corpus contain specialized medical terms. The sublanguage used in each document has been labelled as *lay* or *specialized* by a lay annotator. The corpus is designed as a flexible text resource, where additional medical documents will be appended over time.

The creation of *eCare_Sv_01* stems from the following needs: (1) having a publicly-available medical corpus annotated with lay-specialized labels that can be easily shared; (2) having a corpus with a design and a structure that allow for expansion with additional documents over time; (3) accounting for very specific medical terms.

To date (see Section IV), going to specific websites and

dumping lay-specialized medical texts is what is being normally done. As a matter of fact, these websites do not contain all the illnesses but only the most common ones. The same is true for user-generated texts, such as those that can be found in forums and blogs, since users mostly talk about general problems or common diseases. Another common approach has been to focus on journals or, more rarely, on patient record collections, but in this case there exist copyright, ethical and legal restrictions that limit the shareability and experimental replicability. For all these reasons, with *eCare_Sv_01* we are exploring a different avenue. More specifically, with *eCare_Sv_01* the idea is to pre-select some very specific medical terms (not just the most common illnesses), use them as seeds in a search engine and download only the pages that are related to the specific terms we focus on. In practice, we aim at building a corpus that contains documents that are related **only to specific medical terms** that indicate chronic diseases, and that are not always documented in medical websites, such as the Swedish medical information portal called "1177 Vårdguiden".

As mentioned above, in this paper we describe only preparation work, i.e. the construction of the corpus and present first results. However, the long-term work that leverages on *eCare_Sv_01* include tasks such as: (1) the definition and measurement of the domain-specificity of a corpus (that we call "domainhood"); (2) the automatic extraction of lay-specialized medical lexica and the creation of lexical ontologies from texts that contain specialized terms and lay synonyms; (3) the development of machine-learning-based medical LT applications (e.g. multi-labelled, semi-supervised, weakly-supervised and unsupervised lay-specialized text classification).

The current version of *eCare_Sv_01* contains Swedish web documents related to chronic diseases that are classified as such in the SNOMED CT ontology¹. Since chronic diseases can be treated at home and monitored through electronic devices (sensors, self-reported records, etc.), we intend to use the corpus for LT experiments within the *E-care@home* project (see Section II). In future, the corpus will be expanded with additional diseases (e.g. "tachycardia" or "dementia"), not necessarily classified as chronic in SNOMED CT.

II. LAY-SPECIALIZED MEDICAL TERMINOLOGY AND THE INTERNET OF THINGS

*E-care@home*² is a multi-disciplinary project investigating how to ensure medical care at home and avoid long-term hospitalization in the eldercare. Long hospitalizations are discomforting for elderly patients and expensive for the national healthcare system. Providing medical care at home to the elderly can be effective by populating the home with electronic devices ("things"), i.e. sensors and actuators, and linking them to the Internet. Creating such an Internet-of-Things (IoT) infrastructure is feasible and profitable [1]. Information gathered by sensors are lists of numbers. It is possible however to convert these bare numbers into specialized semantic concepts [2].

This conversion complies to one of *E-care@home* major objectives, i.e. to represent information in a "human consumable way". Converting numbers into concepts expressed in a natural language that experts can understand is certainly a big step forward and it is especially valuable for health professionals, who can use this converted information for timely decision-making. Additionally, since in the *E-care@home* framework patients are empowered and take active part in the management of their illnesses, it is no longer enough to convert sensor data to a medical language that only experts understand. Patients too should be included in the information cycle. There are linguistic obstacles, though. As a matter of fact, medicine is a domain where there exists a divide between the language used by health professionals and the language normally used and understood by patients, caregivers or relatives. This is a well-known problem that is extensively researched (see Section IV). In the project, it is pointed out that: "Patients and citizens will be faced with the technical language of the professional health records. Health care professionals are faced with issues of trustworthiness of personal health record data." Here lies the motivation of *eCare_Sv_01*: the construction of *eCare_Sv_01* exemplifies how to build a concept-specific medical corpus that is useful for eHealth and eCare-oriented LT applications, such as the automatic extraction of lay synonyms corresponding to medical terms.

III. LAY VS SPECIALIZED SUBLANGUAGE

The need of lay synonyms or lay paraphrases that match specialized medical terminology used by healthcare professionals has been the focus of recent research, both in Language Technology [3], and in the clinical community [4]. Research on lay-specialized sublanguages is brought about by the need to improve communication between two specific user groups: the layman on one side, and the expert on the other side. A classical example of a medical term is "varicella", which patients often call "chickenpox". The word "varicella" is a specialized medical term, while "chickenpox" is a lay synonym.

To date, there is no agreed lexical expression that subsumes concepts such as "lay", "normal", "simplified", "expert", "specialized", "consumer health vocabulary", "consumer terminology", and the like. Researchers use different expressions to indicate these kinds of language varieties, for instance, "different genres (such as specialized and lay texts)" [5]; "discourse types (lay and specialized)" [3]; or "registers" [6]. Most commonly, however, researchers do not relate the specialized-lay varieties to any superordinate category, as in [7].

Instead of using an umbrella term like "discourse", or employing textual dimensions like "register" or "genre", we suggest adopting the category **sublanguage** to refer to the different language varieties employed by user groups in certain situational or communicative contexts. Normally, a sublanguage refers to a specialized language or jargon associated with a specific user group, (e.g. the jargon used by teenagers stored in the Corpus of London Teenagers [8]) or to a very specialized domain-specific communication style (e.g. the "notices to skippers"). Computationally, a sublanguage is charac-

¹International SNOMED CT Browser: <http://browser.ihtsdotools.org/>

²Project website: <http://ecareathome.se/>

terized by domain-specific terms (or word co-occurrences) and syntactic cues that deviate from normal language use [9]. We broaden this definition of sublanguage in order to encompass language varieties that are commonly used when two or more user groups communicate in specific domains or in special communicative contexts. Arguably, this definition of sublanguage is unambiguous and applicable to all the domains where the domain-specificity of a jargon causes some kind of "diglossia", and a gap in human communication. Following the extended definition, we can then say that in the medical domain, two sublanguages normally come in contact, namely the **lay sublanguage** used by patients and their relatives (the lay) and the **specialized sublanguage** used by healthcare professionals (the expert).

Normally, lay synonyms are based on everyday language, and are easier to read and to understand than medical terminology, which conversely have high-brow connotation. For normal people without a medical education or background, medical terms are often opaque or hard to remember due the Greek and/or Latin etymology. These terms are called "neo-classical" terms, and, interestingly, recent research shows that also healthcare professionals tend to "normalize" this type of lexicon to everyday language, as in the case of "Swedification" of Latin and Greek affixes in patient records [10]. Generally speaking, it seems that the "layfication" of medical language is an extensive phenomenon that affects, in different ways, several user groups.

IV. PREVIOUS WORK

The automatic identification and extraction of specialized medical terminology and its systematization and standardization is an ongoing effort in many languages. For the Swedish language, experiments show that semi-automatic methods are reliable and can be implemented in real-life settings [11], [12].

Since the focus of our research is on the lay sublanguage rather than on the systematization and standardization of expert terminology, in this section we focus on the latest research on how lay-specialized medical text collections have been designed or used in several languages.

Examples for the English language include a method to mine a lexicon of medical terms and lay equivalents using abstracts of clinical studies and corresponding news stories written for a lay audience [13]. The collection is structured as a parallel corpus of documents for clinicians and for consumers. The study presented in [14] focuses on the linguistic habits of consumers. In this study, the authors empirically evaluate the applicability of their approach using a large data sample consisting of MedLine abstracts as well as posts from a popular online health portal, the MedHelp forum. The "propensity of a term", which is a measure based on the ratio of frequency of occurrence, was used to differentiate consumer terms from professional terms.

For French, experiments have been carried out by [3] to build lay-specialized monolingual comparable corpora using web documents belonging to specific genres from public websites in the medical domain. The corpus devised by [3] is quite

different from *eCare_Sv_01*, since [3] include in their corpus various texts containing any kind of medical terminology, while in the design of *eCare_Sv_01* we only focus on texts related to very specialized illnesses, i.e. those listed under the chronic diseases node in the Swedish SNOMED CT.

In Sweden, research on medical collections is well-established and thriving. For instance, [6] created a unique medical test collection for Information Retrieval to provide the possibility to assess the document relevance to a query according to two user groups, namely patients or doctors. The focus of [7] is on the simplification of one single genre, namely the medical journal genre. To this purpose, the authors used a subset of a collection built from the journal Svenska Läkartidningen, i.e. the Journal of the Swedish Medical association, that was created by [15]. Another unique language resource is the Stockholm EPR (Electronic Patient Records) Corpus [16], [17], which comprises real data from more than two million patient records.

The medical text collections briefly described above are important language resources that, although not always publicly available, can be shared for research purposes under certain conditions. With *eCare_Sv_01*, we are exploring an alternative research path, where a text corpus is purposely designed to be publicly available.

V. THE CORPUS

eCare_Sv_01 is a small text collection bootstrapped from the web. It contains 801 web documents that have been labelled by a *lay annotator*. In the following subsections, we describe its construction and the actual corpus.

A. Seeds

We started off with approximately 1300 term seeds designating chronic diseases in the Swedish SNOMED CT. A qualitative linguistic analysis of the term seeds revealed a wide range of variation as for number of words and syntactic complexity. For instance, multiword terms (n-grams) are much more frequent than single-word terms (unigrams). We counted 13 unigrams (see Table I), 215 bigrams, and the rest of the seeds were characterized by specialized terms and complex syntax, such as: "kronisk inkomplett tetraplegi orsakad av ryggmärgsskada mellan femte och sjunde halskotan" (English: "Chronic incomplete quadriplegia due to spinal cord lesion between fifth and seventh cervical vertebra").

To bootstrap the corpus we used unigrams and bigrams only. This decision was based on the assumptions that (1) unigram- and bigram-terms are more findable on the web than syntactically complex keyword seeds, and (2) complex multiword terms are less likely to have a lay synonym or paraphrase. It should be noticed however that Swedish is a compound language where several words are united in one single graphical unit, so the distinction between unigrams and bigrams is sometimes blurred.

B. Preprocessing and Download

A preliminary investigation showed that when searching for medical terms (the seeds) as search keywords, the list of results

TABLE I
UNIGRAM SEEDS

Seeds (Swedish)	Translation (English)	SCTID
ansiktstics	Facial tic disorder	230335009
bukangina	Abdominal angina	241154007
chalcosis	Chalcosis	46623005
fluoros	Fluorosis	244183009
kromoblastomykos	Chromoblastomycosis	187079000
lipoidnephros	Minimal change disease	44785005
lungemfysem	Pulmonary emphysema	87433001
mycetom	Mycetoma	410039003
ozena	Ozena	69646003
polyserosit	Polyserositis	123598000
postkardiotomi-syndrom	Postcardiotomy syndrome	78643003
Swimmingpool-dermatit	Swimming pool dermatitis	277784005
trumhinneatelektas	Tympanic atelectasis	232258001

contains many irrelevant documents, which make a specialized corpus noisy. We decided to use seeds in the following way. Each seed was used as search keyword in *Google.se* (Google web domain for Sweden). For each seed, Google returned a number of hits. We limited our analysis to hits on the first page. We manually opened each snippet to have an idea of the type of web documents that were retrieved. For each search lap, several documents were irrelevant and several were duplicated. 74 keyword seeds were discarded because the retrieved documents were irrelevant or written in a foreign language. Unsurprisingly, we also noticed that the number of retrieved pages depends on how common a disease is. For instance, "ansiktstics" (English: "facial tics") had many hits, while "chalcosis" (English: "chalcosis") very few. As a rule of thumb, we decided to select a maximum of 20 documents for the most common illnesses, and as many as we could for rarer diseases. After this preprocessing phase, we applied BootCat [18] using the advanced settings (i.e. *url seeds*) to create the web corpus.

We handed out the bootcat-ted documents to a native Swedish speaker (an academic) who does not work in the medical domain and has no medical-related education. The lay annotator proceeded with the labelling by applying a *lay* or *specialized* label to each text in the corpus.

C. *eCare_Sv_01* in a Nutshell

eCare_Sv_01 has been bootstrapped using 228 terms (13 unigrams and 215 bigrams). After the preprocessing, 843 urls (112 for unigrams and 731 for bigrams) were factored out and used as *url-seeds* in BootCat. Some of the urls were automatically discarded by BootCat (e.g. bilingual documents were discarded) and some bootcat-ted documents were empty. Finally, 801 documents were successfully bootcat-ted. Table II shows the corpus statistics.

The annotator pointed out that the writing quality of a number of web documents was poor, mainly because they had been machine translated, and not written by humans. Some of the web documents explicitly stated "Översatt från engelska av

Microsoft" (English: Translated from English by Microsoft). Out of 801 web documents, 339 have received comments by the lay annotator, e.g. "Machine Translated" or "it is about animals and not about humans".

Essentially, we can observe that the corpus is noisy. The annotator's comments help us understand the different types of noise and emphasize a crucial issue that is underexplored in corpus- and computational linguistics, i.e. the reliability and the quality of corpora bootstrapped from the web. The automatic discrimination of "good" documents from "bad" ones is an important problem, especially in sensitive domains like the medical or legal domains. This topic will certainly be explored in our future research. However, in the experiments that we report in this paper we took another perspective and investigated to what extent lay-specialized text classification is robust to noise. Since cleaning a corpus might be prohibitive for a number of reasons, the challenge is to see whether noisy corpora can be used in Language Technology without affecting the performance of LT applications.

For this reasons, the noisy documents have been left in the corpus but they are flagged so they can be easily included or bypassed, according to the purpose of the research, as we did in the experiments presented in Section VII. Other types of research that can benefit from the inclusion of noisy texts in the corpus include the automatic analysis of MT "translationese" [19] and the automatic quality assessment of text writing³.

D. *Web Corpora and Copyright*

Legislation about the copyright and the re-usability of web documents that are not licensed under a Creative Commons Attribution has not been standardized globally. In some countries, regulations exist, but they are supposed to be valid on the national territory. For instance, in the US, the legal doctrine called Fair Use⁴ permits limited use of copyrighted material without acquiring permission from the rights holders. Similarly, in the UK, a recent Exception⁵ (Feb 2016) to the copyright law allows researchers to make copies of copyright material for computational analysis. According to this Exception researchers are given the "Ability to mine all types of content/data". More specifically, "The exception permits any published and unpublished in-copyright works to be copied for the purpose of text mining for non-commercial research. This includes sound, film/video, artistic works, tables and databases, as well as data and text, as long as the researcher has lawful access.". This exception explicitly regulates a lawful behaviour and it is very convenient for researchers.

According to the International Comparative Legal Guides website, in Sweden big data and analytics are permitted⁶.

Unfortunately, to date, in many countries, text and data mining copyright regulations remain implicit rather than explicit. There are practices though that help researchers. One

³Somehow related to this topic is the recently funded project in the UK: "Text-based measures of information quality in online health information".

⁴See https://en.wikipedia.org/wiki/Fair_use

⁵See <https://www.jisc.ac.uk/guides/text-and-data-mining-copyright-exception>

⁶See <https://iclg.com/practice-areas/data-protection/data-protection-2017/sweden#chaptercontent12>

TABLE II
CORPUS STATISTICS

	# initial seeds	# retrieved seeds	# bootCatted URLs	URLs per seed: Mean	URL per seed: Median	URL per seed: SD	# words
Unigr.	13	13	112	8.61	9.3	3.57	91 118
Bigrams	215	142	689	4.85	4	3.16	618 491
Total	228	155	801	5.16	5	3.35	709 609

practice that as been adopted in some contexts is to scramble the content; another approach is to limit the use of the content to a certain number of characters; other practices are described in portals and forums⁷.

As a matter of fact, texts in *eCare_Sv_01* have not been reproduced in their integrity. When BootCat retrieves and downloads a document, it automatically removes boilerplate and other parts of the original web documents. These cleaning procedures facilitate the use of the corpus for automatic text analysis. In practice, this means that some parts of the original web pages have been stripped out from the web documents stored in *eCare_Sv_01* when BootCat preprocessed the documents for the download.

Research-wise, working on a corpus and being unable to share it to allow experimental replication or contrastive analysis is not only frustrating but it also curtails future progress⁸. Since we wish to enlarge *eCare_Sv_01* over time via collective collaboration, *eCare_Sv_01* is made public and is freely available for research purposes. We are ready to remove any text(s) from the corpus upon an objection from its copyright holder, although to our knowledge, nobody has ever requested to remove any web text from collections crawled from the web, neither within the "web as a corpus" experience, nor within the "wacky" initiative, nor with Common Crawl corpus⁹. *eCare_Sv_01* is distributed under the following disclaimer: "Copyright is held by the author/owner(s) of the web documents included in the corpus. The documents in the corpus can be used for research purposes ONLY."

VI. HUMAN ANNOTATION AND INTER-RATER AGREEMENT

The annotation of documents in the corpus as being *lay* or *specialized* was carried out by a native speaker who participates in the project. The lay annotator works in Language Technology and has little knowledge of medical terminology.

To have an idea of the agreement between a lay annotator and an expert annotator, we asked a second annotator who works in Health Informatics to annotate a small sample out of the whole corpus. Then we measured the agreement between the two annotators.

⁷For instance, see <http://linguistics.stackexchange.com/questions/9232/do-i-have-copyright-issues-when-making-a-corpus-from-the-web>

⁸On this topic see also: Branco, A., Cohen, K.B., Vossen, P. et al. "Replicability and reproducibility of research results for human language technology: introducing an LRE special section" Lang Resources & Evaluation 2017 51

⁹See <http://commoncrawl.org/the-data/>

Several inter-rater agreement measures exist [20]. All the inter-rater agreement measures have their strong points and their drawbacks and the use of one over the other depends on the data, the task and the situation. In our case, we wish to measure to what extent two members belonging to two different user groups (i.e. the lay and the expert) spontaneously agree when assessing the difficulty of medical language. Our expectation is that a lay person tends to label as "specialized" a larger number of medical documents than an expert person, who, conversely, tends to see as "lay" many documents that laypeople would consider to be "specialized". In order to test this assumption, we measured the inter-rater agreement by using the classic unweighted Cohen's *kappa* [21] and Krippendorff's *alpha* [22] to get a straightforward indication of the raters' tendencies. Cohen's κ assumes independence of the two coders and is based on the assumption that "if coders were operating by chance alone, we would get a separate distribution for each coder" [20]. This assumption intuitively fits our expectations. Krippendorff's α is similar to Cohen's κ , but it also takes into account the extent and the degree of disagreement between raters [20].

Table III shows the interrater agreement on the annotated texts. Interestingly, annotators tend to disagree more on documents harvested with unigrams (Row 1), while they agree more on documents harvested with bigrams (Row 2). All in all, both κ and α scores are approx. 0.5, and both these values indicate a "moderate" agreement according to the magnitude scale for κ [23], and the α range [24]. These values endorse our hypothesis that there exists a "user group bias". If we contextualize the results, this finding means that patients (who usually have a "lay" perspective) tend to perceive many documents as "specialized", while doctors would assess these documents simply "normal". This has a linguistic implication that affects LT applications in the eHealth field as a whole, and we encourage more in-depth investigation about this topic in the future.

TABLE III
INTER-RATER AGREEMENT VALUES

# documents	Percentage	Cohen's Kappa	Krippendorff's Alpha
112 (unigr. seeds)	75.9	0.52	0.51
236 (bigr. seeds)	82.2	0.60	0.60
348 (all)	80.2	0.57	0.57

VII. SUPERVISED LEARNING: THE LAY PERSPECTIVE

In this section, we present two experiments based on lay-specialized text classification. We apply fully-supervised machine learning methods to explore how well supervised algorithms learn the labels applied by the *lay annotator*.

Experiment 1 focuses on scalability, and help us understand whether the size of the corpus has an impact of the classification results. In Experiment 2, we explore to what extent lay-specialized text classification is affected by noisy documents.

In these experiments, we relied on the Weka Machine Learning Workbench [25] (Explorer and Experimenter interfaces).

A. Quick-and-Dirty: Features and Noisy Texts

The first question to answer when performing lay-specialized text classification is: which features are most appropriate to represent lay and specialized medical sublanguages? Intuitively, one would argue that readability assessment features could well represent the difference between lay and specialized texts. A stable set of readability assessment features is available for Swedish and has been applied to several standard corpora [26]. Unfortunately, texts crawled from the web are noisy, also after being automatically cleaned by BootCat. For instance, texts may contain informal language (e.g. sv: "nå'n annan som hatar utredningen?" English: "somebody else who hates the investigation"), and unpredictable combinations of English words (e.g. "therapycounseling") are numerous. This means that the automatic extraction of readability assessment features from *eCare_Sv_01* would imply a regularization of the corpus that we have not planned yet. At this stage, we focus on how to leverage on noisy texts rather than on how to regularize them. For this reason, we decided to apply a filter that requires no text pre-processing, namely the *StringToWordVector* filter that converts strings (i.e. textual content) to vectors of words. Only two attributes were declared, namely *the textual content of the document* defined as "string", and the *sublanguage label* (either "lay" or "specialized") defined as "nominal".

B. Experiment 1: Lay-Specialized Text Classification and Scalability

We converted four subsets of the whole corpus into four datasets. The first dataset contains 156 documents; the second one 220 documents; the third one 337 documents; the fourth datasets includes the whole corpus and contains 801 documents. The four datasets contain some overlapping data since we wish to simulate the progressive expansion of the corpus over time by appending more documents to the original corpus. The rationale of this experimental setting is to observe whether and to what extent the performance of the classifiers deteriorates when increasing the corpus size.

Since we did not know in advance which type of machine learning modelling would be more suitable for this kind of data, we applied three standard algorithms that have very different inductive biases, namely *Decision Trees*, *Naive Bayes* and *SVM*. We used Weka's implementations of these algorithms, i.e. *J48*, *Naive Bayes* and *SMO*. All the

algorithms were run with standard parameters. We ran each of the algorithms via a metaclassifier (i.e. *Classify - Meta - FilteredClassifiers*) and we selected in turn each of the pre-decided classifiers together with the *StringToWordVector* filter (standard parameters). We applied 10-fold-crossvalidation. Results are shown in Tables IV, V, VI and VII (values have been truncated to two decimal places).

For the first dataset (156 documents), *J48* seems to be less suitable than *Naive Bayes* and *SMO*. *J48*'s k statistic is low, indicating that most of the corrected classifications happen by chance. The confusion matrix for *J48* shows that lay texts are quite confusing for this classifier (only 48 TP vs 35 misclassified cases), while specialized texts are more clearly set apart (110 TP vs 27 misclassifications). *Naive Bayes* and *SMO* do a better job on this dataset: their averaged ROC area values are much higher than 0.5 (0.5 would mean that a classifier is random). On the second dataset (220 documents), *J48*'s performance values are equivalent to *Naive Bayes*'s and *SMO*'s. On the third dataset (337 documents), *SMO* shows better figures. The performance on the fourth dataset is similar to the third dataset.

In order to compare the performance of the three classifiers on the four datasets, we applied the Corrected Paired T-Test (two tailed) provided by Weka's Experimenter interface. Statistical significance was measured on the results of the three classifiers per dataset, and on the performance of each classifier on the four datasets. Statistical significance was measured at significance level of $P < 0.001$ on the weighted averaged F-measure. The test did not detect any statistically significant variation. We interpret these findings as a sign of stability since results show the robustness of the models to scalability issues. This experiment supports our claim that a corpus can be extended without causing any deterioration of the performance of LT applications.

C. Experiment 2: Lay-Specialized Text Classification With and Without Noise

In Experiment 2 we explored whether there exists a performance gap between text classification models trained on a collection containing noisy documents and text classification models trained on a collection containing only noise-less documents.

Results are shown in Table VII and Table VIII respectively. In order to compare the two sets of results, we measured the performance of the same algorithm on the two datasets. As in Experiment 1, statistical significance was measured at significance level of $P < 0.001$ on the weighted averaged F-measure. The test did not detect any statistically significant variation. We interpret these findings as a sign of resistance to noise in the lay-specialized text classification task. This experiment supports our claim that noise does not always negatively affect classification performance.

D. Discussion

Experimental results show that lay-specialized classification performance is good (averaged F-measure is above 0.70 in

TABLE IV
DATASET 1: 156 DOCUMENTS

	k	Acc.	Avg. P	Avg. R	Avg. F	ROC A.	Avg. TP	Avg. FP
J48	0.14	62.8	0.62	0.62	0.62	0.63	0.62	0.42
NB	0.46	75.6	0.77	0.75	0.76	0.80	0.75	0.26
SMO	0.43	75.6	0.75	0.75	0.75	0.71	0.75	0.32

TABLE V
DATASET 2: 220 DOCUMENTS

	k	Acc.	Avg. P	Avg. R	Avg. F	ROC A.	Avg. TP	Avg. FP
J48	0.38	71.8	0.71	0.71	0.71	0.69	0.71	0.33
NB	0.45	72.7	0.75	0.72	0.73	0.78	0.72	0.25
SMO	0.36	70.9	0.70	0.70	0.70	0.67	0.70	0.35

TABLE VI
DATASET 3: 337 DOCUMENTS

	k	Acc.	Avg. P	Avg. R	Avg. F	ROC A.	Avg. TP	Avg. FP
J48	0.38	72.1	0.71	0.72	0.71	0.71	0.72	0.33
NB	0.46	73.5	0.76	0.73	0.74	0.80	0.73	0.23
SMO	0.50	77.1	0.77	0.77	0.77	0.75	0.77	0.27

TABLE VII
DATASET 4: ALL 801 DOCUMENTS

	k	Acc.	Avg. P	Avg. R	Avg. F	ROC A.	Avg. TP	Avg. FP
J48	0.38	74.15	0.74	0.74	0.74	0.66	0.74	0.37
NB	0.45	73.9	0.78	0.73	0.74	0.83	0.73	0.23
SMO	0.49	78.6	0.78	0.78	0.78	0.74	0.78	0.29

most cases) and stable across classifiers and across datasets of different sizes.

In our view these results are promising for two main reasons. The first reason is *scalability*: Experiment 1 shows that results are essentially equivalent across samples of different sizes since we observe no statistically significant degeneration in the performance when scaling out. This is reassuring: we can imagine a scenario where we design a dynamic and extensible corpus whose size can be increased over time, and this will not affect the expectation of efficiency and reliability of LT applications when scaling out.

The second reason is *resilience to noise*: removing noisy documents from a corpus can be prohibitive in some contexts. Arguably, not all LT applications require high quality texts to ensure a good performance and reliable results, as we have shown in Experiment 2.

VIII. CONCLUSIONS AND FUTURE WORK

In this position paper we argued that 1) leveraging on a dynamic and extensible corpus does not necessarily imply scalability issues for LT applications; 2) leveraging on a noisy corpus does not necessarily imply decreases in performance. To support our claims we presented the results of two experiments in lay-specialized text classification using standard algorithms with standard parameters. Results are not only promising but also encouraging because we expect that more

customized algorithms and optimized parameters can improve on the current performance of the classification models.

The paper presents several novelties. The first novelty is the creation of a very specialized web corpus with highly technical terms coming from SNOMED CT (Swedish version). This design is new since, to our knowledge, normally medical web corpora are built using documents related to common diseases (like varicella, measles, etc.) rather than to very specific illnesses.

We introduced the notion of "user group bias", which indicates that lay annotator and the expert annotator tend to disagree when asked to assess whether a document is lay or specialized. Our experience shows that the annotators' judgment is biased towards their own expertise (or lack of expertise) in the medical field. This a new type of awareness that it is worth discussing in future.

Promising findings have been presented about corpus scalability and noise resilience. Corpus scalability implies that a corpus can be increased over time and this will not necessarily affect the performance of LT applications based on that corpus. Noise resilience indicates that it is not always necessary to remove noisy documents from a corpus to get reliable performance. Building LT applications that are resistant to noise is an important future direction in Language Technology. Another LT application that may remain unaffected by the noise-ness of corpus is automatic lexicon induction based

TABLE VIII
DATASET WITHOUT NOISY TEXTS: 462 DOCUMENTS

	k	Acc.	Avg. P	Avg. R	Avg. F	ROC A.	Avg. TP	Avg. FP
J48	0.36	72.29	0.72	0.72	0.72	0.69	0.72	0.35
NB	0.57	79.22	0.82	0.79	0.79	0.88	0.79	0.16
SMO	0.57	80.95	0.81	0.81	0.81	0.78	0.81	0.23

on distributional semantics, where the emphasis is on the contextual similarity rather than on the quality of writing style. We will test this assumption in future experiments.

Currently we are working on the definition of statistical measures that help us gauge the degree of domain-specificity (i.e. the "domainhood") of a corpus with respect to a general-purpose corpus.

Future work includes the expansion of the corpus with texts in other languages and related to diseases not necessarily classified as chronic in SNOMED CT, e.g. "tachycardia" or "dementia". Additionally, since the current version of *eCare_Sv01* is small, we plan to expand it also by relying on semi-supervised and weakly supervised learning.

ACKNOWLEDGMENTS

Thanks to all the reviewers of the manuscript who, with their feedback, helped improve the original draft. Thanks to Wiktor Strandqvist who contributed to the experiments with R scripts. Corpus, scripts and the output of the classification models are available from the project website: <http://ecareathome.se>. We encourage the replication of the results presented in this paper, and welcome improvements and further discussion. This research was funded by the distributed environment Ecare@Home funded by the Swedish Knowledge Foundation.

REFERENCES

- [1] M. Alirezaie, H. Karl, and B. Eva, "A pattern language for smart home applications," *Semantic Web*, vol. 00, no. 00, p. 00, 2017.
- [2] M. Alirezaie, "Bridging the semantic gap between sensor data and ontological knowledge," Ph.D. dissertation, Örebro university, 2015.
- [3] L. Deléger, B. Cartoni, and P. Zweigenbaum, "Paraphrase detection in monolingual specialized/lay corpora," *Building and Using Comparable Corpora*, 2013.
- [4] M. Sedor, K. J. Peterson, L. A. Nelsen, C. Cocos, J. B. McCormick, C. G. Chute, and J. Pathak, "Incorporating expert terminology and disease risk factors into consumer health vocabularies," in *Pacific Symposium on Biocomputing. Pacific Symposium on Biocomputing*. NIH Public Access, 2013, p. 421.
- [5] L. Deléger and P. Zweigenbaum, "Extracting lay paraphrases of specialized expressions from monolingual comparable medical corpora," in *Proceedings of the 2nd Workshop on Building and Using Comparable Corpora: from Parallel to Non-parallel Corpora*. Association for Computational Linguistics, 2009, pp. 2–10.
- [6] K. F. Heppin, "Resolving power of search keys in medieval a swedish medical test collection with user groups: Doctors and patients," Ph.D. dissertation, Ph. D. thesis, University of Gothenburg, 2010.
- [7] E. Abrahamsson, T. Forni, M. Skeppstedt, and M. Kvist, "Medical text simplification using synonym replacement: Adapting assessment of word difficulty to a compounding language," in *Proceedings of the 3rd Workshop on Predicting and Improving Text Readability for Target Reader Populations (PIITR)@ EACL*, 2014, pp. 57–65.
- [8] V. Haslerud and A.-B. Stenström, "The bergen corpus of london teenager language (colt)," *Spoken English on computer*, pp. 235–42, 1995.
- [9] R. Basili, M. T. Paziienza, and P. Velardi, "Acquisition of selectional patterns in sublanguages," *Machine Translation*, vol. 8, no. 3, pp. 175–201, 1993.
- [10] G. Grigonytė, M. Kvist, M. Wirén, S. Velupillai, and A. Henriksson, "Swedification patterns of latin and greek affixes in clinical text," *Nordic Journal of Linguistics*, vol. 39, no. 01, pp. 5–37, 2016.
- [11] M. Nyström, M. Merkel, L. Ahrenberg, P. Zweigenbaum, H. Petersson, and H. Åhlfeldt, "Creating a medical english-swedish dictionary using interactive word alignment," *BMC medical informatics and decision making*, vol. 6, no. 1, p. 35, 2006.
- [12] M. Nyström, M. Merkel, H. Petersson, and H. Åhlfeldt, "Creating a medical dictionary using word alignment: the influence of sources and resources," *BMC medical informatics and decision making*, vol. 7, no. 1, p. 37, 2007.
- [13] N. Elhadad and K. Sutaria, "Mining a lexicon of technical terms and lay equivalents," in *Proceedings of the Workshop on BioNLP 2007: Biological, Translational, and Clinical Language Processing*. Association for Computational Linguistics, 2007, pp. 49–56.
- [14] V. V. Vydiswaran, Q. Mei, D. A. Hanauer, and K. Zheng, "Mining consumer health vocabulary from community-generated text," in *AMIA Annual Symposium Proceedings*, vol. 2014. American Medical Informatics Association, 2014, p. 1150.
- [15] D. Kokkinakis, "The journal of the swedish medical association—a corpus resource for biomedical text mining in swedish," in *The Third Workshop on Building and Evaluating Resources for Biomedical Text Mining (BioTextM), an LREC Workshop. Turkey*, 2012.
- [16] H. Dalianis, M. Hassel, and S. Velupillai, "The stockholm epr corpus—characteristics and some initial findings," *Women*, vol. 219, no. 906, p. 54, 2009.
- [17] H. Dalianis, A. Henriksson, M. Kvist, S. Velupillai, and R. Weegar, "Health bank—a workbench for data science applications in healthcare," in *CAiSE Industry Track*, 2015, pp. 1–18.
- [18] M. Baroni and S. Bernardini, "Bootcat: Bootstrapping corpora and terms from the web," in *LREC*, 2004.
- [19] V. Volansky, N. Ordan, and S. Wintner, "On the features of translationese," *Digital Scholarship in the Humanities*, vol. 30, no. 1, pp. 98–118, 2015.
- [20] R. Artstein and M. Poesio, "Inter-coder agreement for computational linguistics," *Computational Linguistics*, vol. 34, no. 4, pp. 555–596, 2008.
- [21] J. Cohen, "A coefficient of agreement for nominal scales," *Educational and psychological measurement*, vol. 20, no. 1, pp. 37–46, 1960.
- [22] K. Krippendorff, "Content analysis. beverly hills," *California: Sage Publications*, vol. 7, pp. 1–84, 1980.
- [23] J. Sim and C. C. Wright, "The kappa statistic in reliability studies: use, interpretation, and sample size requirements," *Physical therapy*, vol. 85, no. 3, p. 257, 2005.
- [24] K. Krippendorff, "Computing krippendorff's alpha-reliability," 2011. [Online]. Available: http://repository.upenn.edu/asc_papers/43
- [25] I. H. Witten, E. Frank, M. A. Hall, and C. J. Pal, *Data Mining: Practical machine learning tools and techniques*. Morgan Kaufmann, 2016.
- [26] J. Falkenjack, K. H. Mühlenbock, and A. Jönsson, "Features indicating readability in swedish text," in *Proceedings of the 19th Nordic Conference of Computational Linguistics (NODALIDA 2013); May 22-24; 2013; Oslo University; Norway. NEALT Proceedings Series 16*, no. 085. Linköping University Electronic Press, 2013, pp. 27–40.

10th International Workshop on Computational Optimization

MANY real world problems arising in engineering, economics, medicine and other domains can be formulated as optimization tasks. These problems are frequently characterized by non-convex, non-differentiable, discontinuous, noisy or dynamic objective functions and constraints which ask for adequate computational methods.

The aim of this workshop is to stimulate the communication between researchers working on different fields of optimization and practitioners who need reliable and efficient computational optimization methods.

TOPICS

The list of topics includes, but is not limited to:

- combinatorial and continuous global optimization
- unconstrained and constrained optimization
- multiobjective and robust optimization
- optimization in dynamic and/or noisy environments
- optimization on graphs
- large-scale optimization, in parallel and distributed computational environments
- meta-heuristics for optimization, nature-inspired approaches and any other derivative-free methods
- exact/heuristic hybrid methods, involving natural computing techniques and other global and local optimization methods

The applications of interest are included in the list below, but are not limited to:

- classical operational research problems (knapsack, traveling salesman, etc)
- computational biology and distance geometry
- data mining and knowledge discovery
- human motion simulations; crowd simulations
- industrial applications
- optimization in statistics, econometrics, finance, physics, chemistry, biology, medicine, and engineering.

BEST PAPER AWARD

The best WCO'17 paper will be awarded during the social dinner of FedCSIS 2017.

The best paper will be selected by WCO'17 co-Chairs by taking into consideration the scores suggested by the reviewers, as well as the quality of the given oral presentation.

SECTION EDITORS

- **Fidanova, Stefka**, Bulgarian Academy of Sciences, Bulgaria
- **Mucherino, Antonio**, INRIA, France
- **Zaharie, Daniela**, West University of Timisoara, Romania

REVIEWERS

- **Bonates, Tibérius**, Universidade Federal do Ceará, Brazil
- **Breaban, Mihaela**
- **Chira, Camelia**, Technical University of Cluj-Napoca, Romania
- **Gonçalves, Douglas**, Universidade Federal de Santa Catarina, Brazil
- **Hosobe, Hiroshi**, Hosei University, Japan
- **Iiduka, Hideaki**, Kyushu Institute of Technology, Japan
- **Lavor, Carlile**, IMECC-UNICAMP, Brazil
- **Marinov, Pencho**, Bulgarian Academy of Science, Bulgaria
- **Micota, Flavia**, West University of Timisoara, Romania
- **Muscalagiu, Ionel**, Politehnica University Timisoara, Romania
- **Parsopoulos, Konstantinos**, University of Ioannina, Greece
- **Pintea, Camelia**, Tehnical University Cluj-Napoca, Romania
- **Roeva, Olympia**, Institute of Biophysics and Biomedical Engineering, Bulgaria
- **Siarry, Patrick**, Universite Paris XII Val de Marne, France
- **Stefanov, Stefan**, South-West University "Neofit Rilski, Bulgaria
- **Stoean, Ruxandra**
- **Stoean, Catalin**
- **Stuetzle, Thomas**, Université Libre de Bruxelles (ULB), Belgium
- **Tamir, Tami**, The Interdisciplinary Center (IDC), Israel
- **Zilinskas, Antanas**, Vilnius University, Lithuania

On Pathological Fitness Landscapes for Constrained Combinatorial Optimization

Gary Greenfield
 Mathematics and Computer Science
 University of Richmond
 Richmond, Virginia 23173
 Email: ggreenfi@richmond.edu

Aldeida Aleti
 Faculty of Information Technology
 Monash University
 Melbourne, Victoria, Australia
 Email: aldeida.aleti@monash.edu

Abstract—Population-based search methods such as evolutionary algorithms follow gradients in the fitness landscape under the assumption that high quality solutions will lead to even better ones. Most real-world optimisation problems, however, have constraints which lead to infeasible solutions that may disrupt these gradients. As a result, high quality solutions may lie in regions that are often unreachable from regions in the fitness landscape where the preponderance of feasible solutions lie. In such cases, the make-up of the initial population as well as critical aspects of the search strategy become the crucial factors in determining whether or not high quality regions are ever reached. In this paper, we present examples of pathological landscapes that arise by considering the constrained component deployment optimisation problem for which standard evolutionary algorithms are almost certain to fail to reach the regions where high quality solutions lie. We indicate how some simple modifications can help alleviate this problem.

I. INTRODUCTION

The typical oral presentation of an evolutionary algorithm paper might include a fitness landscape slide such as the one shown in Figure 1. This tends to lull the listener into thinking that standard exploitation and exploration computation techniques will successfully explore the landscape encountering some number of local minima and maxima and, hopefully, eventually a global minimum or maximum.

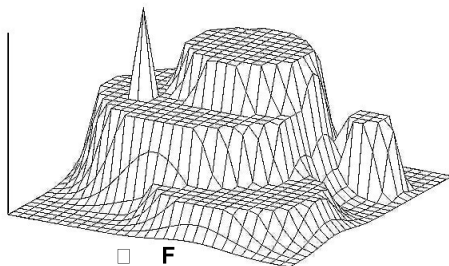


Fig. 1. A typical presentation slide for visualizing what the underlying fitness landscape for a combinatorial optimisation problem might look like.

Of course, this will not be true in general, but this trust becomes particularly misleading for problems where there are regions in the search space of the fitness function where fitness is undefined. The objective of this paper is to present examples inspired by a constrained combinatorial optimisation problem

that highlight some of the pathologies that can arise in such situations and to suggest some simple “fixes” which might avoid these difficulties.

II. BACKGROUND

A. Evolutionary Algorithms

In combinatorial optimisation *evolutionary algorithms* are iterative methods that evolve a population of solutions determined by *genomes* through the use of mutation, crossover, and selection operators. The optimisation process starts with a set of randomly generated genomes as an initial population. At every iteration, mutation and crossover operators are applied to some portion of the population.

The proportion of the population that is used for “reproduction” first undergoes crossover, which combines parts of two parent genomes to create two new genomes. A 1-point crossover splits both genomes at one point and combines the respective genes. It is possible to split solutions at more than one position, known as k -point crossover, and interleave the results. The points where the crossovers occur are selected at random. Next, the newly created solutions are mutated at a certain rate. There are various types of mutation operators: 1-point mutation mutates only one gene in the genome, uniform mutation mutates each gene with a certain probability, and transposition mutation operators swap two different genes in the same genome. Note that while 1-point and uniform mutation operators may alter existing genes, the transposition mutation operator can only change the position of genes. Hence, only 1-point and uniform mutation operators can introduce new genes not already in the population.

The selection operator decides which solutions will survive to the next iteration and adds new genomes as determined above in order to maintain the specified population size. Depending on the evolutionary approach, the selection can be based on elitism (only the best solutions survive), quality proportionate (the probability that a solution survives is based on its fitness), or random. We refer to mutation, crossover, and selection as search operators.

B. Fitness Landscapes

The suitability of an evolutionary method for solving an optimisation problem instance depends on the structure of the

fitness landscape of that instance. A fitness landscape in the context of constrained combinatorial optimisation problems is a setting comprising all of the following:

- a search space S of all possible genomes
- an ordered set V of fitness values
- a fitness function $F : S \rightarrow V$
- a set of constraints Ω
- a feasible set $S' \subset S$ satisfying all $\omega \in \Omega$,
- an infeasible set $I \subset S$ violating at least one $\omega \in \Omega$,
- a neighbourhood relation $N(s) \subset S$ for each $s \in S$

An example of a neighbourhood relation determined by 1-point mutation is the relation which assigns as neighbours to a genome all genomes that differ in one gene. A neighbourhood relation could also be specified by applying crossover with another genome, usually a genome restricted to lie in some subset of S , followed by mutation.

C. The Software Deployment Problem

Aleti [1] considers a combinatorial optimisation problem that seeks to assign $n \geq 3$ software components c_1, \dots, c_n to $m \geq 3$ hardware devices h_1, \dots, h_m subject to certain constraints in such a way that a fitness function that measures “reliability” is maximized once a *deployment* function $d : C \rightarrow H$, where C is the set of components and H is the set of hardware units, is specified. Thus, subject to the constraints, once c_1 has been deployed to $d(c_1)$, c_2 to $d(c_2)$, and so forth fitness can be evaluated. But because of the constraints, not all candidate deployment functions $d : C \rightarrow H$ are valid and thus the domain of feasible solutions for the fitness landscape has an unknown (and possibly unknowable) topology.

This context provided the inspiration for considering how difficult it might be to come up with a simple instance where “holes” in the domain might guarantee that absolute maxima would never be found using (standard) evolutionary search methods. In other words, we are looking for what would essentially be a minimal counterexample. Our attempts are described in the following sections.

III. A MINIMAL COUNTEREXAMPLE

For a positive integer v , let Z_v denote the set $\{1, \dots, v\}$. We modify the formulation of the component deployment optimisation problem slightly by writing the deployment function as $a : Z_n \rightarrow Z_m$ so that c_1 gets assigned to $h_{a(1)}$, c_2 to $h_{a(2)}$, and so forth. In this way our fitness functions can be viewed as being defined on genomes that are vectors with n components *i.e.*, on n -tuples of the form $(a(1), \dots, a(n))$, where $1 \leq a(i) \leq m$ for all i . This convention will facilitate counting in the sequel. Note that as n -tuples genotypes can be visualized as paths on the bounded region of the integer lattice given by $\{(x, y) \in Z \times Z | 1 \leq x \leq n, 1 \leq y \leq m\}$ by representing $(a(1), \dots, a(n))$ as the path connecting the sequence of points $(1, a(1)), \dots, (n, a(n))$.

Our constraints will be: c_1 cannot be deployed to h_m , or equivalently $a(1) < m$; c_n cannot be deployed to h_m , or equivalently $a(n) > 1$; and c_1 can be deployed to h_1 if and only if c_n is deployed to h_m , or equivalently $a(1) = 1$ if

and only if $a(n) = m$. This last constraint is the critical constraint used to isolate a subset of assignment functions where maximal fitness solutions will lie. Our constraints are listed in Table I.

Constraints
$a(1) < m$
$a(n) > 1$
$a(1) = 1$ if and only if $a(n) = m$

TABLE I
CONSTRAINTS ON n -TUPLE GENOMES $(a(1), \dots, a(n))$ WHERE
 $1 \leq a(i) \leq m$ FOR ALL i .

Our minimal counterexample takes $n = m = 3$, the first nontrivial case, so that of the twenty-seven possible 3-tuples that are potential candidates for a 's only six satisfy the constraints, namely those of the form $(2, *, 2)$ or $(1, *, 3)$ where $*$ represents a “wild card” character that can assume any value chosen from the set $Z_3 = \{1, 2, 3\}$. Suppose the fitness function F satisfies $F((1, *, 3)) = 4$, $F((2, *, 2)) = 1$, and is undefined for any of the remaining twenty-one 3-tuples that do not satisfy the constraints. The six feasible solutions when represented as paths are shown in Figure 2.

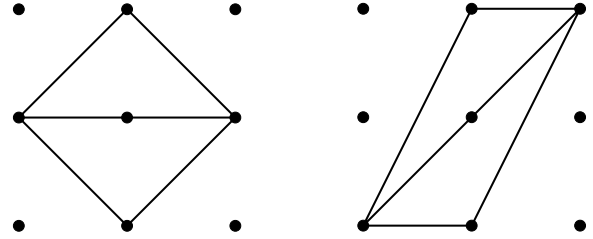


Fig. 2. The paths for our minimal counterexample.

Let our evolutionary method have population size $s = 3$, and suppose that none of the three 3-tuples that have maximal fitness make it into the initial population. That is, the initial population contains only genomes of the form $(2, *, 2)$. Then, regardless of whether one is using 1-point or 2-point crossover no genome produced by recombining two genomes in the current population will ever have maximal fitness. Further, if we use as a mutation operator single point mutation (*i.e.*, we change only one of the components) or we use a swap operator that interchanges two components, this is still the case. In fact, in a population of $(2, *, 2)$ genomes, crossover followed by either a one-point mutation or a swap will also fail to ever yield a maximal fitness genome of the form $(1, *, 3)$. In order for evolutionary computation to succeed for our toy problem when the initial population consists of only $(2, *, 2)$ genomes it must implement an operator that yields a swap combined with a one-point mutation or a mutation operator that perturbs two or more components *i.e.* a two-point mutation operator. It is also curious to note that if a global maximum is obtained by, say, a swap combined with a one-point mutation, then the genome must be $(1, 2, 3)$. Interestingly, the evolutionary algorithm used for the software deployment problem in Sabar

and Aleti [2] does implement a swap followed by a point mutation, however it checks the validity of the genome after the swap which would cause it to fail for our toy problem.

IV. SCALING THE COUNTEREXAMPLE

The reason our counterexample is so intriguing is because it generalizes and scales to a constrained combinatorial optimization problem with more plausible parameters. Using the same constraints, assume now that $m, n \geq 3$. Then the domain of candidate assignment functions consists of the m^n n -tuples with entries in $Z_m = \{1, \dots, m\}$. We shall be fluid in referring to elements in this search space as n -tuples, candidates, solutions, genomes or points. We partition the set of candidates into three disjoint subsets: high quality feasible candidates Q , low quality feasible candidates B , and infeasible candidates I . Q consists of n -tuples of the form $(1, *, \dots, *, m)$ of which there are m^{n-2} . B consists of n -tuples of the form $(X, *, \dots, *, Y)$, where $1 < X, Y < m$ of which there are $(m-2)m^{n-2}(m-2)$. I consists of the remaining n -tuples. I also decomposes into disjoint sets. These disjoint sets together with their cardinalities are shown in Table II. We can check that this decomposition is correct by observing that we have accounted for all n -tuples as follows:

$$m^{n-2}[1 + (m-2)^2 + 4(m-2) + 3] = m^n.$$

Set	Cardinality
$(1, *, \dots, *, Y)$	$(m-2)m^{(n-2)}$
$(X, *, \dots, *, m)$	$(m-2)m^{(n-2)}$
$(m, *, \dots, *, Y)$	$(m-2)m^{(n-2)}$
$(X, *, \dots, *, 1)$	$(m-2)m^{(n-2)}$
$(m, *, \dots, *, 1)$	$m^{(n-2)}$
$(1, *, \dots, *, 1)$	$m^{(n-2)}$
$(m, *, \dots, *, m)$	$m^{(n-2)}$

TABLE II

DECOMPOSITION OF SET OF I OF INFEASIBLE n -TUPLE GENOMES INTO DISJOINT SUBSETS. X AND Y ASSUME VALUES BETWEEN 2 AND $m-1$ WHILE $*$ IS A WILD CARD CHARACTER INDICATING ANY VALUE BETWEEN 1 AND m INCLUSIVE IS ALLOWED.

Our counting also tells us that when choosing an n -tuple at random, the probability of getting a feasible solution is $[(m-2)^2 + 1]/m^2$ and the probability of getting a candidate from B or I , a candidate that does *not* satisfy the condition $a(1) = 1$ if and only if $a(n) = m$, is $1 - (1/m^2)$. This makes it easy to determine the probability of randomly selecting genomes one at a time and winding up with an initial population of genomes lying exclusively in $B \cup I$ (see below).

It is more difficult to obtain a closed form expression for the probability that a an initial population where n -tuples are selected one by one, with infeasible solutions *discarded*, until a population (possibly with duplicates) of size s is obtained such that it contains only feasible solutions from B *i.e.*, only feasible solutions that don't have $a(1) = 1$ and $a(n) = m$. Let p_Q, p_B and p_I be the probabilities that a randomly chosen genome lies in Q, B and I respectively. We know

$$p_Q = 1/m^2, p_B = (1 - 2/m)^2, p_I = (4m - 5)/m^2.$$

For fixed $j \geq s$, let p_j be the probability of getting a pool with s genomes from B after randomly choosing exactly j genomes. Then we know the last genome must have been from B and $s-1$ genomes from B must have shown up in the previous $j-1$ selections. Since there are $\binom{j-1}{s-1}$ ways for genomes from B to get selected, knowing the remaining $j-s$ choices all came from I , we have

$$p_k = \left[\binom{j-1}{s-1} p_B^{s-1} p_I^{j-s} \right] p_B,$$

whence the desired probability is:

$$\begin{aligned} \sum_{j=s}^{\infty} p_k &= p_B^s \sum_{j=s}^{\infty} \binom{j-1}{s-1} p_I^{j-s} \\ &= p_B^s \sum_{j=s}^{\infty} \frac{s}{j} \binom{j}{s} p_I^{j-s} \\ &= p_B^s \sum_{k=0}^{\infty} \frac{s}{s+k} \binom{s+k}{s} p_I^k \\ &= (1 - 2/m)^{2s} \sum_{k=0}^{\infty} \frac{s}{s+k} \binom{s+k}{s} \left(\frac{4m-5}{m^2} \right)^k. \end{aligned}$$

If we are willing to accept infeasible solutions in the initial population, but require our fitness functions to assign positive values for feasible solutions and zero for infeasible solutions so that they will immediately be removed from the initial population, then we can assert that the probability of an initial population *not* having a feasible solution from Q , (*i.e.*, not having a genome of the form $(1, *, \dots, *, m)$) is $(1 - (1/m^2))^s$. Note that when $m = 10$ and $s = 100$ this probability already exceeds one-third. We assume an initial population of this type for the remainder of this paper. This assumption, coupled with more realistic parameter values, for example $s = 100$ and $m, n \geq 10$, allows us to formulate some additional pathological fitness landscape examples. We first digress to a discussion of search operators.

A. Search operators

For notation, we let X_i denote the 1-point crossover that occurs at position i where $1 < i < n$. Formally, for genomes a_1 and a_2 , this means

$$\begin{aligned} X_i((a_1(1), \dots, a_1(n)), (a_2(1), \dots, a_2(n))) = \\ ((a_1(1), \dots, a_1(i-1), a_2(i), \dots, a_2(n)), \\ (a_2(1), \dots, a_2(i-1), a_1(i), \dots, a_1(n))). \end{aligned}$$

For $1 \leq i \leq n$ and $1 \leq j \leq m$, we let $P_{i,j}$ denote the point mutation operator that assigns $a(i)$ to be j . For $1 \leq i < j \leq n$ we define $T_{i,j}$ to be the transposition operator that swaps $a(i)$ with $a(j)$.

B. Simple Scaling

Assume $m, n \geq 3$, the initial population contains solutions only from B and I , and the fitness function F is defined by setting $F((a(1), \dots, a(n)))$ equal to 0, 1, and $m+1$ for

solutions from I , B , and Q respectively. Then, assuming that solutions from I are immediately removed from the population and only low quality solutions from B remain available for recombination and selection to form the next generation, remarks similar to the minimal counterexample apply. No single application of any $P_{i,j}$ or $T_{i,j}$ to a genome can produce a high quality solution from a low quality solution. This is still true even if they are applied to an intermediate genome arising from composition of a sequence of crossover operators.

However, such a “lifting” from B to Q will occur whenever $P_{1,1} \circ P_{m,m}$ is applied to a genome in B . If we posit a typical scenario where uniform point mutation is used, which is interpreted to mean that components are considered one by one so that, independently, each has probability p that a point mutation operator is applied, then for fixed i and j , the i -th component has probability p/m of having $P_{i,j}$ applied and the probability $P_{1,1}$ and $P_{n,m}$ are both applied is $(p/m)^2$. Note that for $p = 0.05$ and $m = 10$ this probability is 0.000025. Another possible way for such a lifting to occur is if a genome has $a(i) = m$ and $a(j) = 1$ where $1 < i, j < m$ — assume this occurs with probability ρ — and the composition of $T_{1,j}$ with $T_{i,m}$ (they are disjoint transpositions, so the order doesn’t matter) is applied. Since there are $n(n-1)/2$ transposition operators, if there is some (small) probability ϵ of applying two swaps to a genome of the desired type, then the probability of a successful lifting is $4\rho\epsilon/(n^2 - n)$.

C. Biasing Low Quality Solutions

We can make it harder for liftings from B to Q to occur by arranging it so that the percentage of genomes with 1’s and m ’s in interior components within a population consisting of genomes only from B decreases as the evolutionary algorithm progresses. That is, over time we can try to lower the value of ρ . Define the *target* t to be $\lfloor \frac{m+1}{2} \rfloor$. Note that $t = 2$ when $m = 3$, and that $1 < t < m$, for $m \geq 3$.

Assume the initial population consists of only candidates from B and I . As before, let genomes in I and Q have fitness 0 and $m+1$, but now for $(a(1), \dots, a(n)) \in B$ set

$$F((a(1), \dots, a(n))) = 1 + \prod_{i=1}^n \frac{1}{|a(i) - t| + 2}.$$

Observe that these fitness values all lie strictly between 1 and 2. This biases the evolutionary algorithm such that as evolution proceeds an initial population consisting of genomes only from B and I converges to one consisting entirely of the unique local minimum solution (t, \dots, t) which has fitness $1 + 1/2^n$.

D. Biasing High Quality Solutions

Finally, we can immediately expel all but a select few high quality genomes that do creep into the population as a result of liftings from B to Q by lowering their fitness as follows.

Assume the initial population consists of only candidates from B and I . Let genomes in I and B have fitness 0 and 2 respectively. If $(1, a(2), \dots, a(n-1), m) \in Q$, let u be minimal such that $a(1) = \dots = a(u) = 1$ and $a(u+1) \neq 1$. Note that u is well defined and $1 \leq u < m$. Define

$F(1, a(2), \dots, a(n-1), m) = 1/(1+u)$ if $(1, a(2), \dots, a(n-1), m) \neq (1, m, \dots, m)$ and $m+1$ otherwise. This fitness function immediately removes all genomes lifted from B to Q except for the global maximum $(1, m, \dots, m)$ which has fitness $m+1$ by ensuring they have fitness less than one.

V. DISCUSSION — PART 1

It is of course possible to simplify the fitness functions in our examples. We decided to use more involved fitness terms, terms that without closer inspection might more easily pass for those one might expect to encounter in “real-world” applications, to try and promote plausibility.

The critical constraint we rely on may seem far fetched, but in highly constrained scheduling problems with large numbers of variables that are overseen by systems using evolutionary techniques, it can certainly be the case that a complex set of constraints winds up inducing simple or unusual constraints like ours without anyone consciously realizing it. Our best effort at formulating a problem instance where our constraints might make sense runs as follows. Assume mission critical or fail safe software processes c_1, \dots, c_n are currently running on hardware processors h_2, \dots, h_{m-1} in a real time system. Suppose that processors h_1 and h_m are now to be brought online while processes c_1 and c_n are upgraded such that for load balancing purposes c_1 should migrate to h_1 but cannot migrate to h_m and, similarly, c_n should migrate to h_m but cannot migrate to h_1 .

If one does accept our thesis that fitness landscapes with pathological topologies can lead to situations where standard evolutionary algorithms are bound to fail, then as a byproduct of our examples we have an argument in favor of adopting a richer set of mutation operators, especially those that promote repeated applications of point mutation or transposition.

VI. RELATED WORK

In this section we consider related work on the relationship between fitness landscapes and optimisation problems. Unfortunately, most of the work considers only *unconstrained* optimisation. For comprehensive surveys of empirical approaches to characterising fitness landscapes see Malan [3] and Pitzer [4].

A. Models

Several different models for fitness landscapes have been proposed in the literature including additive fitness landscapes [5], random fitness landscapes [6], the block model [7], and the NK model [8]. Additive fitness landscapes are single peaked. In contrast, in a random fitness landscape there is no correlation between the fitnesses of mutational neighbours, hence such landscapes are considered rugged and tend to have many peaks. In the block model, the genotype is composed of blocks of genes which independently contribute to the overall fitness *i.e.*, the fitness of the genotype depends on the contribution from each block. The NK model comprises genotypes with N genes. It depends on the parameter K , where $K \leq N-1$, signalling that the fitness contribution of

each gene depends on its interactions with a block of K other genes. Thus K also serves as an indicator of the ruggedness of the fitness landscape.

B. Time to Convergence

Another related avenue of research is using Markov chain theory to analyse the behaviour of evolutionary algorithms and predict how long it will take for a Markov chain representing the different states reached in the search space (e.g., the search space history) to achieve stationarity. Hernandez *et al.* [9] use coupling from the past to detect time to convergence, while Propp *et al.* [10] propose a sampling algorithm based on the idea of coupling. Since, in theory, reaching stationarity requires infinite time, Propp and Wilson provide an algorithm that can detect when stationarity has been reached in finite time. Their work was later extended by Hernandez [9].

C. Problem Hardness

Much of the theoretical work relating fitness landscapes to problem hardness has taken place within the context of biological or evolutionary landscapes. Organismal biologists seek to understand the physical, biochemical and physiological basis of genotype to phenotype mappings, while evolutionary biologists study evolutionary causes and consequences. In these situations what matters most is whether the landscape is rugged or smooth and the degree of epistasis (the interaction between genes that are not alleles [11]) occurring in genomes.

In combinatorial optimisation, features of the fitness landscape that may have an impact on problem hardness have been estimated empirically using fitness landscape characterisation metrics [12]. These features pertain to the existence of local optima, global optima, and plateaus. Assuming the optimization objective is maximisation, given a search space S and a neighbourhood relation N , a local optimum occurs at a point $s_l \in S$ if for any solution $s_n \in N(s_l)$, $F(s_l) \geq F(s_n)$. A global optimum occurs at a point $s_g \in S$ if for all $s \in S$, $F(s_g) \geq F(s)$. A plateau is defined as a set $P \subseteq S$ such that for all $s_p \in P$, $F(s_p) = k$, where k is a constant. (A technical condition for ensuring *connectedness* is also needed, but it will not concern us here.) A plateau indicates that the landscape is neutral, and the progress of a gradient-based search algorithm, such as an evolutionary algorithm, potentially stagnates. Counteracting such stagnation requires special measures (see, for example, Barnett [13]).

Landscape modality also figures into problem hardness. Modality is a feature of fitness landscapes that encompasses the number of local optima, the distribution of the points where they occur, and the nature of their respective basins of attraction [14]. In a search space S equipped with neighborhood relation, a local optimum s_l , the basin of attraction for s_l is defined as the set of all $s \in S$ such that there is a hill climb starting at s that ends at s_l . More precisely, a *path* in S is a finite sequence s_1, \dots, s_k in S such that $s_{i+1} \in N(s_i)$ for $1 \leq i < k$ and a hill climb from s to s_l is a path such that $s_1 = s$, $s_k = s_l$ and $F(s_{i+1}) \geq F(s_i)$ for $1 \leq i < k$. The number of basins of attraction and their

relative sizes in a multi-modal landscape have been found to determine how difficult it is for a gradient-based search algorithm to find a global optimum among all the local optima it encounters (see Horn [15]). While on one hand finding global optima in unimodal problems can be difficult if plateaus dominate the landscape, on the other hand in some highly multi-modal landscapes it can be easy to find global optima for both hill-climbing algorithms and evolutionary algorithms if, for example, the modes themselves “lean” towards a global optimum.

Ruggedness is another feature that has been found to affect the performance of gradient-following algorithms. An optimisation problem is considered easier to solve using either local search or an evolutionary algorithm if highly correlated parts of the landscape form easy-to-follow gradients to the optima [16]. As mentioned previously, in rugged landscapes neighbouring solutions have uncorrelated fitnesses which makes it harder for a search method to infer a search direction from previous solution quality. When the landscape is smoother and the correlation between the fitnesses of neighbouring solutions is high, there are persistent gradients (i.e., long paths) for the solver to follow. Because there is little correlation between neighbouring solutions, gradients in a rugged fitness landscape are not persistent which, in turn, suggests numerous local optima.

VII. DISCUSSION — PART 2

The literature in the previous section on theoretical and empirical investigations of fitness landscapes and their relationship to optimisation problems is focused on problems without constraints. It provides a backdrop for providing further insight into our examples. Our search space S is a finite set of n -tuples and the neighborhood relation of interest is 1-point mutation, so $N(s) = \{P_{i,j}(s_n) | 1 \leq i \leq n, 1 \leq j \leq m\}$. This equips S with the edit distance metric, where two points are a distance k apart if they differ in exactly k positions or, in our notation, if one can be transformed into the other using a k -fold composition of 1-point mutations.

For our minimal counterexample the high quality solutions Q of the form $(1, *, 3)$ and the low quality solutions B of the form $(2, *, 2)$ are plateaus. Their genomes can be viewed as parallel lines in the $3 \times 3 \times 3$ lattice cube. These lines are edit distance two apart. The four parallel lines that are edit distance one from $(2, *, 2)$ (viz. $(2, *, 1)$, $(2, *, 3)$, $(1, *, 2)$, $(3, *, 2)$) all lie in the infeasible region I . Figure 3 shows a schematic of this. More importantly, in *all* of our examples k -fold crossover is closed on both Q and B . That is every k -fold crossover operator takes $Q \times Q$ to itself and $B \times B$ to itself. Hence searching in any direction from B does not reach genomes in Q unless search operators such as 2-fold mutation operators (e.g., 2-point mutation) or doubly transitive permutation operators (e.g., 2-fold transposition or a transposition composed with a 1-point mutation) are introduced.

Our three scaled examples increase the size of B relative to Q and also do a better job of filling out the search space with feasible solutions, meaning as m and n increase the ratio of the

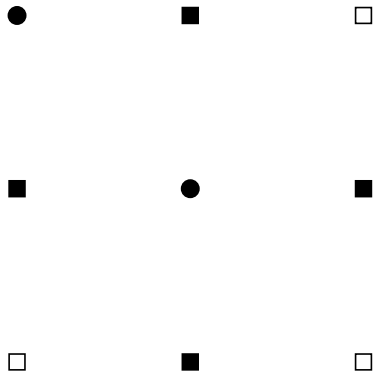


Fig. 3. A schematic showing the endpoints in the xz -plane of the nine parallel lines of the form $(x_0, *, z_0)$ for the $n = m = 3$ case. The filled circles are the two lines of feasible solutions (upper left is Q , center is B). The squares are the seven lines of infeasible solutions. The filled squares show the four lines that are edit distance one from B .

size of $Q \cup B$ to the size of I increases. Genomes in Q and B continue to remain at least edit distance two apart. In example IV-B, Q and B remain plateaus. In example IV-C, Q remains a plateau while B becomes a basin of attraction for the local minimum (t, t, \dots, t) where $t = \lfloor \frac{m+1}{2} \rfloor$. In example IV-D, B remains a plateau while Q has a global maximum occurring when the genome is $(1, m, \dots, m)$. The situation in IV-D is a bit more complicated than that. There is a putative local maximum of $1/2$ at all genomes of the form $(1, Z, *, \dots, *, m)$ except $(1, m, \dots, m)$, where $2 \leq Z \leq m$, and a basin of attraction for one of them has been “punctured” in such a way that $(1, m, \dots, m)$ yields the isolated global maximum. Since B is a plateau every genome in B yields a local maximum, so another way to phrase what is happening is to say, all the local maxima, putative or otherwise, of Q save one are smaller than all the local maxima of B .

Finally, if our quest was for a minimal counterexample, the reader may wonder why we didn’t use just the constraint $a(1) = 1$ if and only if $a(3) = 3$ which, using our lines notation, would enlarge the pool of base solutions from $B = \{(2, *, 2)\}$ to $B = \{(2, *, 2), (2, *, 1), (3, *, 1), (3, *, 2)\}$. There are two reasons. First, this would admit the possibility of the transposition operator $T_{1,3}$ lifting a genomes of the form $(3, *, 1)$ from B to Q . Second, this would increase the number of “subspaces” invariant under crossover so that populations with genomes restricted to B , any one of the lines in B , or any pair of lines in B' that agree in one coordinate (e.g., $\{(2, *, 2), (3, *, 2)\}$) would all be invariant under crossover.

VIII. CONCLUSION

We have considered how pathological fitness landscapes affect the success of evolutionary algorithms in finding global optima in constrained optimisation problems. We formulated examples to show how constraints can shape fitness landscapes

in such a way that regions of high quality solutions become unreachable from regions of lower quality solutions when using the standard search operators. Our examples stem from the software deployment problem. We presented a minimal counterexample and generalized it to provide several examples with real-world parameters as well as a more plausible narrative for the problem instances. The unexpected byproduct is that our examples provide a compelling argument for including iterated transposition and iterated point mutation among the set of search operators when using evolutionary algorithms to find solutions to highly constrained optimization problems.

REFERENCES

- [1] A. Aleti, “Designing automotive embedded systems with adaptive genetic algorithms,” *Automated Software Engineering*, vol. 22, no. 2, pp. 199–240, 2015. doi: 10.1007/s10515-014-0148-0
- [2] N. R. Sabar and A. Aleti, “An adaptive memetic algorithm for the architecture optimisation problem,” in *Australasian Conference on Artificial Life and Computational Intelligence*. Springer, 2017. doi: 10.1007/978-3-319-51691-2_22 pp. 254–265.
- [3] K. M. Malan and A. P. Engelbrecht, “A survey of techniques for characterising fitness landscapes and some possible ways forward,” *Information Sciences*, vol. 241, pp. 148–163, 2013. doi: 10.1016/j.ins.2013.04.015
- [4] E. Pitzer and M. Affenzeller, “A comprehensive survey on fitness landscape analysis,” *Studies in Computational Intelligence*, vol. 378, pp. 161–191, 2012. doi: 10.1007/978-3-642-23229-9_8
- [5] R. Mani, R. P. S. Onge, J. L. Hartman, G. Giaefer, and F. P. Roth, “Defining genetic interaction,” *Proceedings of the National Academy of Sciences*, vol. 105, no. 9, pp. 3461–3466, 2008. doi: 10.1073/pnas.0712255105
- [6] S.-C. Park and J. Krug, “Evolution in random fitness landscapes: the infinite sites model,” *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2008, no. 04, p. P04014, 2008. doi: 10.1088/1742-5468/2008/04/P04014
- [7] A. S. Perelson and C. A. Macken, “Protein evolution on partially correlated landscapes,” *Proceedings of the National Academy of Sciences*, vol. 92, no. 21, pp. 9657–9661, 1995. doi: 10.1073/pnas.92.21.9657
- [8] S. A. Kauffman and E. D. Weinberger, “The nk model of rugged fitness landscapes and its application to maturation of the immune response,” *Journal of theoretical biology*, vol. 141, no. 2, pp. 211–245, 1989. doi: 10.1016/S0022-5193(89)80019-0
- [9] G. Hernandez, K. Wilder, F. Nino, and J. Garcia, “Towards a self-stopping evolutionary algorithm using coupling from the past,” in *Proceedings of the 2005 conference on Genetic and evolutionary computation*. ACM, 2005. doi: 10.1145/1068009.1068112 pp. 615–620.
- [10] J. G. Propp and D. B. Wilson, “Exact sampling with coupled markov chains and applications to statistical mechanics,” *Random structures and Algorithms*, vol. 9, no. 1-2, pp. 223–252, 1996. doi: 10.1002/(SICI)1098-2418(199608/09)9:1/2<223::AID-RSA14>3.0.CO;2-O
- [11] R. A. Fisher, “The correlation between relatives on the supposition of mendelian inheritance,” *Transactions of the royal society of Edinburgh*, vol. 52, no. 02, pp. 399–433, 1919. doi: 10.1017/S0080456800012163
- [12] I. Moser, M. Gheorghita, and A. Aleti, “Identifying features of fitness landscapes and relating them to problem difficulty,” *Evolutionary computation*, 2016. doi: 10.1162/EVCO_a_00177
- [13] L. Barnett, “Netcrawling-optimal evolutionary search with neutral networks,” in *Proceedings of the 2001 Congress on Evolutionary Computation*, vol. 1, 2001. doi: 10.1.1.32.9203 pp. 30–37.
- [14] J. Garnier and L. Kallel, “Efficiency of local search with multiple local optima,” *SIAM Journal on Discrete Mathematics*, vol. 15, pp. 122–141, 2002. doi: 10.1137/S0895480199355225
- [15] J. Horn and D. Goldberg, “Genetic algorithm difficulty and the modality of fitness landscapes,” in *Foundations of Genetic Algorithms*, 1994. doi: 10.1.1.31.3340 pp. 243–269.
- [16] P. Stadler and W. Schnabl, “The landscape of the traveling salesman problem,” *Physics Letters A*, vol. 161, pp. 337 – 344, 1992. doi: 10.1016/0375-9601(92)90557-3

Computer Science & Systems

CSS is a FedCSIS conference area aiming at integrating and creating synergy between FedCSIS events that thematically subscribe to more technical aspects of computer science and related disciplines. The CSNS area spans themes ranging from hardware issues close to the discipline of computer engineering via software issues tackled by the theory and applications of computer science and to communications issues of interest to distributed and network systems. Events that constitute CSNS are:

- CANA'17—10th Computer Aspects of Numerical Algorithms
- C&SS'17—th International Conference on Cryptography and Security Systems
- CPORA'17—2nd Workshop on Constraint Programming and Operation Research Applications
- MMAP'17—10th International Symposium on Multimedia Applications and Processing
- WAPL'17—6th Workshop on Advances in Programming Languages
- WSC'17—9th Workshop on Scalable Computing

2nd Workshop on Constraint Programming and Operation Research Applications

THE aim of the CPORA-Workshop on Constraint Programming and Operation Research Applications is to bring together interested researchers from constraint programming/constraint logic programming (CP/CLP), operations research (OR) and artificial intelligence (AI) to present new techniques or new applications in decision support, combinatorial optimization, modeling and control processes arising in manufacturing, transportation, telecommunication, computer networks, logistic systems etc. and to provide an opportunity for researchers in one area to learn about techniques in the others. The aim of this workshop is share ideas, projects, researches results, models, experiences etc. associated with CP/CLP/OR/AI and to give researchers the opportunity to show how the integration of techniques from different fields can lead to interesting results on large and complex problems. Additionally, we would like to stimulate the communication between researchers working on different fields and practitioners who need reliable and efficient modelling and computational methods for industrial and business processes.

Contributions containing of both: the theoretical and practical results obtained in this area are welcome.

TOPICS

- Constraint programming/Constraint logic programming,
- Mathematical programming,
- Constraint Satisfaction Problem,
- Logic programming,
- Hybrid methods,
- Network programming,
- Petri-Nets,
- Knowledge methods,
- Soft computing (FL, GA, NN etc.),
- Answer Set Programming (ASP),
- The boolean satisfiability problem (SAT).

- Manufacturing,
- Multimodal processes management,
- Project management,
- Supply chain management,
- Modeling and planning production flow,
- Production scheduling,
- Multimodal social networks,
- Intelligent transport and passenger routing,
- Network knowledge modeling,
- Transportation networks.

SECTION EDITORS

- **Bocewicz, Grzegorz**, Koszalin University of Technology, Poland
- **Sitek, Pawel**, Kielce University of Technology, Poland

REVIEWERS

- **Banaszak, Zbigniew**, Warsaw University of Technology, Poland
- **Burduk, Anna**, Wrocław University of Science and Technology, Poland
- **Bzdyra, Krzysztof**, Koszalin University of Technology
- **Gola, Arkadiusz**, Lublin University of Technology, Poland
- **Janardhanan, Mukund Nilakantan**, Aalborg University, Denmark, Denmark
- **Nielsen, Peter**, Aalborg University, Denmark
- **Nielsen, Izabela Ewa**, Aalborg University, Denmark
- **Ratnayake, Chandima**
- **Terkaj, Walter**, ITIA-CNR, Italy
- **Turkyilmaz, Ali**, Nazarbayev University, Kazakhstan
- **Wikarek, Jarosław**, Kielce University of Technology, Poland

An example of the satisfiability problem in the continuous structure

Marek Balcer

Institute of Mathematics, Silesian University of Technology
 Kaszubska 23, 44-100 Gliwice, Poland
 Email: Marek.Balcer@polsl.pl

Abstract—The paper presents and demonstrates the theorem showing the equivalence of the problem of the verifiability test of a logical expression in the discrete model \mathfrak{N} of the logic with the search for the minimum value of a continuous function generated by this expression in the structure \mathfrak{M} , which is a simple extension of \mathfrak{N} . Theoretical considerations are illustrated by the example of a certain semi-heuristic algorithm seeking the minimum value of function φ with a short statistics of its.

I. INTRODUCTION

MANY efficient algorithms have been developed for satisfiability testing. Many of them are presented and classified by Jun Gu in [1]. One branch of this classification includes algorithms namely continuous and constrained algorithms. Its' idea depends on creating multidimensional function which interpolates or approximates some Boolean formulas or logic expressions. The satisfiability problem of these formulas is changed to searching the minimum or the maximum of constructed functions. For example, in 1998 Back et al. proposed to transform SAT into continuous optimisation [3]. Similarly, this method is also used for other satisfiability problems like Max-Sat, Uni-SAT etc. [2]. Replacing the problem of satisfiability with the problem of finding the minimum value of the objective function allows us to use many well-known standard or heuristic optimization algorithms. However, in order to make the algorithms working more effectively it is necessary to make some changes in their design.

In this article particle swarm approach is used to logic systems development, where proposed application is used to model logic system with the search for the minimum value of a continuous function generated for expressions formulated in a predefined structure.

II. MATHEMATICAL BACKGROUND

A. Language

LET \mathcal{L} be the set of all logical expressions formed from the symbols of atomic formulas (atoms) and the logical symbols \sim, \wedge, \vee defined as follows [4]:

If we take the non-empty finite set of $At(\mathcal{L}) = \{p, q, r, \dots\}$ as a set of atoms, then:

\mathcal{L} is the smallest set such that:

1) $At(\mathcal{L}) \subset \mathcal{L}$

2) For any $A, B \in \mathcal{L}$

$$\sim A \in \mathcal{L}$$

$$A \wedge B \in \mathcal{L}$$

$$A \vee B \in \mathcal{L}$$

i.e. $(p \wedge q) \vee (\sim p \vee q) \in \mathcal{L}$

For constructing language we can also use the parenthesis free notation which has better properties for decomposition of expressions [6].

B. Structure

A structure \mathfrak{N} is $\mathfrak{N} = \langle X, f_{\sim}, f_{\wedge}, f_{\vee} \rangle$ where X is a non-empty set called a range of assignment and

$$\begin{aligned} f_{\sim} &: X \rightarrow X, \\ f_{\wedge} &: X \times X \rightarrow X, \quad f_{\vee} : X \times X \rightarrow X, \end{aligned}$$

will be certain functions defined in the domain X and $X \times X$.

C. Assignment

Let Z be a subset of the set of expressions \mathcal{L} . Let us denote the set of all atoms occurring in expressions from the set Z by $At(Z)$.

Definition 1: The assignment in the set X of atomic sets of Z is every function \mathbf{w} , which assigns the atomic proposition of the set Z to the set of X .

Definition 2: The value of an expression A for assignment \mathbf{w} is the element of the set X , obtained by the function $f_{\sim}, f_{\wedge}, f_{\vee}$ from the values assigned by the function \mathbf{w} for atomic proposition evaluated from the expression A .

To illustrate this definition, let's take the following shortcut: $W(\mathbf{w}, A) = \text{expression value } A \text{ for assignment } \mathbf{w}$ [5]

1) (I CONDITION). IF A is an atom, then

$$W(\mathbf{w}, A) = \mathbf{w}(A).$$

2) (INDUCTION CONDITIONS).

$$\begin{aligned} W(\mathbf{w}, \sim A) &= f_{\sim}(W(\mathbf{w}, A)), \\ W(\mathbf{w}, A \wedge B) &= f_{\wedge}(W(\mathbf{w}, A), W(\mathbf{w}, B)), \\ W(\mathbf{w}, A \vee B) &= f_{\vee}(W(\mathbf{w}, A), W(\mathbf{w}, B)), \end{aligned}$$

If the symbols of atoms are in order $At(\mathcal{L}) = \{p_1, p_2, \dots, p_m\}$ then assignment \mathbf{w} can be a vector $\mathbf{w} = (\mathbf{w}(p_1), \mathbf{w}(p_2), \dots, \mathbf{w}(p_m))$

D. Satisfiability

Let $\mathfrak{N} = \langle X, f_{\sim}, f_{\wedge}, f_{\vee} \rangle$ be a structure.

In a set X we can distinguish a non-empty subset T .

Definition 3: (Generalized concept of truth in the structure) The expression A is called T -expression in the structure \mathfrak{N} , if for any assignment in this structure the value of the expression A belongs to the set T .

E. Function generated by the expression

Definition 4: The function generated by the expression A in the \mathfrak{N} structure is called the function

$$\varphi_{\mathfrak{N}}^A : X^m \rightarrow X$$

that, for any assignment \mathbf{w}

$$\varphi_{\mathfrak{N}}^A(\mathbf{w}(p_1), \mathbf{w}(p_2), \dots, \mathbf{w}(p_m)) = W(\mathbf{w}, A),$$

where p_1, p_2, \dots, p_m are all atoms in A .

Example 2.1: Let be given a non empty set of expressions $Z \subset \mathcal{L}$ comprised by the use of operators \sim, \wedge, \vee . Let $\mathfrak{N} = \langle X, f_{\sim}, f_{\wedge}, f_{\vee} \rangle$ be a structure, where $X = \{0, 1\}$ and

$$f_{\sim}(x) = 1 - x,$$

$$f_{\wedge}(x, y) = xy, \quad f_{\vee}(x, y) = \max(x, y),$$

$$\mathfrak{N} = \langle \{0, 1\}, 1 - x, xy, \max(x, y) \rangle.$$

Then, for $A = \lceil (p \wedge q) \vee (\sim p \wedge q) \rceil$

$$\varphi_{\mathfrak{N}}^A(x, y) = \max(xy, (1 - x)y)$$

F. Normal form

Definition 5: The expression A is in a disjunctive normal form if and only if A is an alternative of a finite number of conjunctions A_1, A_2, \dots, A_n , so as

$$A = A_1 \vee A_2 \vee \dots \vee A_n$$

Members of the conjunction A_i are atoms or negation of atoms, so as

$$A_i = B_i^1 \wedge B_i^2 \wedge \dots \wedge B_i^{k_i}$$

where $B_i^j = \lceil p \rceil$ or $\lceil \sim p \rceil$, for p as an element from the set $At(A)$.

If expression A is composed as presented above, then we say that it is of a class $[n, k]$, where

$$k = \max_{i=1 \dots n} k_i$$

Example 2.2: Let $A = \lceil (p \wedge q \wedge r) \vee (p \wedge (\sim q)) \vee ((\sim p) \wedge q \wedge r) \vee (r \wedge s) \vee (p \wedge (\sim r) \wedge s) \rceil$.

Expression A is in the normal disjunctive form class $[5, 3]$. $At(A) = \{p, q, r, s\}$.

Let $\mathfrak{N} = \langle \{0, 1\}, 1 - x, xy, \max(x, y) \rangle$

Having the following assignment \mathbf{w}

$$\mathbf{w}(p) = x_1, \mathbf{w}(q) = x_2, \mathbf{w}(r) = x_3, \mathbf{w}(s) = x_4$$

and using assumption $\max(x, \max(y, z)) = \max(x, y, z)$ function $\varphi_{\mathfrak{N}}^A$ takes the form

$$\varphi_{\mathfrak{N}}^A(x_1, x_2, x_3, x_4) = \max(x_1 x_2 x_3, x_1(1 - x_2), (1 - x_1)x_2 x_3, x_3 x_4, x_1(1 - x_3 x_4))$$

In classical logic it is true that for any expression A there exists an A' expression in the normal form such that

$$A \equiv A'$$

Consequently, further consideration of this article will only be restricted to the examination of expressions in the normal form.

III. FROM DISCRETE TO CONTINUOUS UNIVERSE

Let the structure be given

$$\mathfrak{N} = \langle \{0, 1\}, 1 - x, xy, \max(x, y) \rangle$$

Let us create a new structure by changing only the set X from $\{0, 1\}$ to $\langle 0, 1 \rangle \subset \mathbf{R}$.

$$\mathfrak{M} = \langle \langle 0, 1 \rangle, 1 - x, xy, \max(x, y) \rangle$$

Let A be an expression in the normal form of class $[n, k]$ and $|At(A)| = m$.

Theorem 1: The expression A is a tautology if and only if

$$\varphi_{\mathfrak{M}}^A(x) \geq \frac{1}{2^k}$$

for all $x \in \langle 0, 1 \rangle^m$.

This means that in the continuous structure \mathfrak{M} T -expressions are the $\langle \frac{1}{2^k}, 1 \rangle$ expressions or $R+$ expressions.

In order to prove the above theorem, we first show the truth of several properties of the function $\varphi_{\mathfrak{M}}^A$.

Let's presume the following assumptions.

Let A be an expression from language \mathcal{L} in the normal form class $[n, k]$, where $At(A) = \{p_1, p_2, \dots, p_m\}$, so that

$$A = A_1 \vee A_2 \vee \dots \vee A_n \quad (1)$$

where

$$A_i = B_i^1 \wedge B_i^2 \wedge \dots \wedge B_i^{k_i} \quad (2)$$

and for $1 \leq i \leq n, 1 \leq j \leq k_i$ $B_i^j = \lceil p \rceil$ or $\lceil \sim p \rceil, p \in \{p_1, p_2, \dots, p_m\}$

$$k = \max_{i=1 \dots n} k_i$$

Let us accept at the same time for any $i(1 \leq i \leq m), x_i = w(p_i)$.

Corollary 1: For any $(x_1, x_2, \dots, x_m) \in \{0, 1\}^m$

$$\varphi_{\mathfrak{M}}^A(x_1, x_2, \dots, x_m) \in \{0, 1\}.$$

Corollary 2: If for any $(x_1, x_2, \dots, x_m) \in \{0, 1\}^m$

$$\varphi_{\mathfrak{M}}^A(x_1, x_2, \dots, x_m) = 1.$$

and only if A is a tautology.

The above properties result directly from the structure extension from \mathfrak{N} to \mathfrak{M} .

Corollary 3:

$$\varphi_{\mathfrak{M}}^A\left(\frac{1}{2}, \frac{1}{2}, \dots, \frac{1}{2}\right) = \frac{1}{2^l},$$

where $l = \min_{i=1..n} k_i$.

Lemma 1: If for any $(x_1, x_2, \dots, x_m) \in \langle 0, 1 \rangle^m$

$$\varphi_{\mathfrak{M}}^A(x_1, x_2, \dots, x_m) > 0$$

then A is a tautology.

Proof 1: Let $x = (x_1, x_2, \dots, x_m) \in \{0, 1\}^m$. From the assumption results $\varphi_{\mathfrak{M}}^A(x_1, x_2, \dots, x_m) > 0$. Then from corollary 1 $\varphi_{\mathfrak{M}}^A(x_1, x_2, \dots, x_m) = 1$, so using corollary 2 A is a tautology.

Let us proof **theorem 1**.

(\Leftarrow) If for any $x = (x_1, x_2, \dots, x_m) \in \langle 0, 1 \rangle^m$ $\varphi_{\mathfrak{M}}^A(x) \geq \frac{1}{2^k}$, that $\varphi_{\mathfrak{M}}^A(x) > 0$. Using lemma 1. A is a tautology.

(\Rightarrow) Let A be a tautology and let $x = (x_1, x_2, \dots, x_m) \in \langle 0, 1 \rangle^m$. Let us create a new vector of assignment $\epsilon = (\epsilon_1, \epsilon_2, \dots, \epsilon_m) \in \langle 0, 1 \rangle^m$ that

$$\epsilon_i = \begin{cases} 0 & \text{if } x_i \leq \frac{1}{2} \\ 1 & \text{if } x_i > \frac{1}{2} \end{cases} \quad \text{for } i = 1 \dots m \quad (3)$$

Because $\epsilon = (\epsilon_1, \epsilon_2, \dots, \epsilon_m) \in \{0, 1\}^m$ therefore using corollary 2

$$\varphi_{\mathfrak{M}}^A(\epsilon_1, \epsilon_2, \dots, \epsilon_m) = 1.$$

Using (1) A is in a form

$$A = A_1 \vee A_2 \vee \dots \vee A_n$$

Therefore

$$\varphi_{\mathfrak{M}}^A = \max(\varphi_{\mathfrak{M}}^{A_1}, \varphi_{\mathfrak{M}}^{A_2}, \dots, \varphi_{\mathfrak{M}}^{A_n})$$

Because $\varphi_{\mathfrak{M}}^A(\epsilon) = 1$, then must exist $i(1 \leq i \leq n)$ that $\varphi_{\mathfrak{M}}^{A_i}(\epsilon) = 1$.

Using (2),

$$A_i = B_i^1 \wedge B_i^2 \wedge \dots \wedge B_i^{k_i},$$

and therefore

$$\varphi_{\mathfrak{M}}^{A_i} = \varphi_{\mathfrak{M}}^{B_i^1} \varphi_{\mathfrak{M}}^{B_i^2} \dots \varphi_{\mathfrak{M}}^{B_i^{k_i}}$$

Because $\epsilon = (\epsilon_1, \epsilon_2, \dots, \epsilon_m) \in \{0, 1\}^m$ for any $j(1 \leq j \leq k_i) \varphi_{\mathfrak{M}}^{B_i^j}(\epsilon) = 1$ using corollary 1 and assumption $\varphi_{\mathfrak{M}}^{A_i}(\epsilon) = 1$.

Because $B_i^j = \lceil p \rceil$ or $\lceil \sim p \rceil$, where $p \in \{p_1, p_2, \dots, p_m\}$ for $1 \leq i \leq n, 1 \leq j \leq k_i$, therefore exist $t(1 \leq t \leq m)$ that

$$\varphi_{\mathfrak{M}}^{B_i^j} = \begin{cases} w(p_t) & \text{if } B_i^j = \lceil p_t \rceil \\ 1 - w(p_t) & \text{if } B_i^j = \lceil \sim p_t \rceil \end{cases}$$

Because $\varphi_{\mathfrak{M}}^{B_i^j}(\epsilon) = 1$, therefore $\varphi_{\mathfrak{M}}^{B_i^j}(\epsilon_t) = 1$.

$$\varphi_{\mathfrak{M}}^{B_i^j}(\epsilon_t) = \begin{cases} \epsilon_t & \text{if } B_i^j = \lceil p_t \rceil \text{ or when } \epsilon_t = 1 \\ 1 - \epsilon_t & \text{if } B_i^j = \lceil \sim p_t \rceil \text{ or when } \epsilon_t = 0 \end{cases}$$

Therefore

$$\varphi_{\mathfrak{M}}^{B_i^j}(x_t) = \begin{cases} x_t & \text{if } \epsilon_t = 1 \\ 1 - x_t & \text{if } \epsilon_t = 0 \end{cases}$$

Because $x_t > \frac{1}{2}$ when $\epsilon_t = 1$ and $x_t \leq \frac{1}{2}$ when $\epsilon_t = 0$ using construction (3) so

$$\varphi_{\mathfrak{M}}^{B_i^j}(x_t) \geq \frac{1}{2}$$

and further for any $i(1 \leq i \leq n)$

$$\varphi_{\mathfrak{M}}^{A_i}(x) = \varphi_{\mathfrak{M}}^{B_i^1} \varphi_{\mathfrak{M}}^{B_i^2} \dots \varphi_{\mathfrak{M}}^{B_i^{k_i}} \geq \frac{1}{2^{k_i}}$$

Because

$$\varphi_{\mathfrak{M}}^A = \max(\varphi_{\mathfrak{M}}^{A_1}, \varphi_{\mathfrak{M}}^{A_2}, \dots, \varphi_{\mathfrak{M}}^{A_n}), \text{ that}$$

$$\varphi_{\mathfrak{M}}^A(x) \geq \varphi_{\mathfrak{M}}^{A_i}(x) \geq \frac{1}{2^{k_i}} \geq \frac{1}{2^k}, \text{ where } k = \max_{i=1..n} k_i$$

what ends the proof of the theorem.

This theorem demonstrates that the satisfiability test of a logical expression in the discrete model of logic \mathfrak{N} is equivalent to finding extremum of the continuous function φ in the area $\langle 0, 1 \rangle^m$ generated by that expression in the structure \mathfrak{M} . Summing up, we are looking for the smallest value of a function knowing that it is 0 in the case that its generating statement is false or greater than 0 when the expression is true, with additional information about its lower limit resulting from the above statement.

Using the mathematical analysis of continuous property we know that the smallest value of a function can be realized at the points of its extremes inside the examined area or on its border.

Since every expression in the normal class $[n, k]$ ($k > 3$) can be reduced to a task in the form of a normal class $[n_1, 3]$ for $n_1 > n$, where numerical tests are reduced to testing only this class.

TABLE I
BENCHMARK TESTING - NUMBER OF ITERATIONS DEPENDING M AND N

M \ N	30	35	40	45
8	10.66	16.35	20.15	25.35
10	10.13	18.46	34.02	46.79
12	6.52	15.52	32.58	59.21
14	5.19	12.05	25.00	47.67

IV. SOME NUMERICAL EXPERIMENTS

In order to test the effectiveness of the developed method of investigating the fulfillment of logical expressions with the function generated by the expression, the following algorithm was used. Algorithm in pseudo-code

data:

m - the number of atomic formulas which can built A

n - the number of conjunctives in A

k - the number of atomic formulas in each conjunctive

s - the number of particles,

T_{max} - maximal number of iterations

Generate random (testing) formula A in a normal form of the class $[n, k]$ Generate random particles x_1, x_2, \dots, x_s

```

while  $t < T_{max}$  do
2: Evaluate  $\varphi^A(x_1), \varphi^A(x_2), \dots, \varphi^A(x_s)$ 
   Find minimum of  $\{\varphi^A(x_1), \varphi^A(x_2), \dots, \varphi^A(x_s)\}$ 
4: if minimum  $< \frac{1}{2^k}$  then
   A is "false"; stop
6: end if
   Create new particles  $x_1, x_2, \dots, x_s$  by PSO method
8: end while

```

Classic PSO method [7] build new particles (for $i = 1 \dots s$)

$$x_i^{new} = x_i^{old} + \alpha(x_{max}^{old} - x_i^{old}) + \beta(t)random([0, 1]^m),$$

where α and $\beta(t)$ are moderating coefficients.

Results of testing this algorithm in original classic version of PSO were unsatisfied. Only some random cases were positive. More of tests were divergent.

After many experiments one of the best has the following form.

If $x_i^t = (x_{i,1}^t, x_{i,2}^t, \dots, x_{i,m}^t)$ is an old position of particle that construction of new particle is (for $l = 1 \dots m$)

$$x_{i,l}^{new} = \begin{cases} 1 - \beta(t)rnd[0, 1] & \text{if } x_{i,l}^{old} < \frac{1}{2} \\ 0 + \beta(t)rnd[0, 1] & \text{if } x_{i,l}^{old} \geq \frac{1}{2} \end{cases}$$

when $\varphi(x_i^{old}) \geq \varphi(x_{best}^{old})$.

We can also accelerate the process if one or more of the started particles are $(\frac{1}{2}, \frac{1}{2}, \dots, \frac{1}{2})$.

Since each expression in the normal form $[n, k]$ ($k > 3$) can be reduced to an expression in the form of a normal class $[n_1, 3]$, where $n_1 > n$ numerical tests are reduced to testing only class ($k = 3$).

Hint: It is also good if the number of particles is equal of the number of atomic formulas. ($m = s$) After these changes we have the next statistic results of constructed algorithm.

The array represents the average amount of iterations after which the algorithm identifies the expression as non-satisfiability. Parameters of this statistics are:

M - the number of atoms in the tested expression

N - the number of alternative members i.e. the number of different triple conjunctions (clauses) in the expression.

Tests were performed for randomly generated 1000 false statements for each pair of parameters.

V. CONCLUSION

Equivalence of SAT examinations - a discrete problem in the \mathfrak{N} model with the search for the minimum value of the continuous function φ in the \mathfrak{M} structure opens the way to using heuristic algorithms to solve both problems. The problem, however, is to find an effective algorithm, which briefly signals the example discussed above. This, however, opens up a wide field for further research both in constructing new algorithms and for finding other discrete structures and their continuous extensions similar to those presented in the article.

Looking from another perspective, the functions generated by logical statements can become very demanding test functions for evaluating heuristic algorithms.

We can also risk the assertion that, similarly to the discrete-matter classification, it is also possible to classify the functions of the NP class as exemplified by the functions of the class NP, which are examples of functions generated by expressions and others that are difficult to judge at the current level of research.

REFERENCES

- [1] Jun Gu "The Multi-SAT algorithm," *Discrete Applied Mathematics*, vol.96-97 pp. 111-126, 1999 Elsevier Science B.V.,doi:10.1016/S0166-218X(99)00035-9.
- [2] R. Battiti, M. Protasi, "Approximate Algorithms and Heuristics for MAX-SAT," *Handbook of Combinatorial Optimization*(vol.1)pp.77-148, 1998 Kluwer Academic Publisher, doi:10.1007/978-1-4613-0303-9-2.
- [3] J. Gottlieb, E. Marchiori, C. Rossi, "Evolutionary Algorithms for the Satisfiability Problem," *Evolutionary Computation*, vol 10(1) MITP 2002, doi:10.1162/106365602317301763.
- [4] J. Malitz, "Introduction to Mathematical Logic," *Undergraduate Text in Mathematics*, Springer Verlag 1979 New York
- [5] K. Grzegorzczuk, "Zarys Logiki Matematycznej," *Biblioteka Matematyczna*, PWN 1985 Warszawa
- [6] M. Balcer, "Characteristics and decomposition of expressions in the PF-notation," *Silesian Journal of Pure and Applied Mathematics*, vol.6 is.1(2016) pp.5-22
- [7] J. Kennedy, R. Eberhart, "Particle Swarm Optimization," *Proceedings of IEEE International Conference on Neural Networks*, vol.IV pp. 1942-1948, doi:10.1109/ICNN.1995.488968.

6th Workshop on Advances in Programming Languages

PROGRAMMING languages are programmers' most basic tools. With appropriate programming languages one can drastically reduce the cost of building new applications as well as maintaining existing ones. In the last decades there have been many advances in programming languages technology in traditional programming paradigms such as functional, logic, and object-oriented programming, as well as the development of new paradigms such as aspect-oriented programming. The main driving force was and will be to better express programmers' ideas. Therefore, research in programming languages is an endless activity and the core of computer science. New language features, new programming paradigms, and better compile-time and run-time mechanisms can be foreseen in the future.

The aims of this event is to provide a forum for exchange of ideas and experience in topics concerned with programming languages and systems. Original papers and implementation reports are invited in all areas of programming languages.

TOPICS

- Automata theory and applications
- Compiling techniques
- Context-oriented programming languages to specify the behavior of software systems and dynamic adaptations
- Domain-specific languages
- Formal semantics and syntax
- Generative and generic programming
- Grammarware and grammar based systems
- Knowledge engineering languages, integration of knowledge engineering and software engineering
- Languages and tools for trustworthy computing
- Language theory and applications
- Language concepts, design and implementation
- Markup languages (XML)
- Metamodeling and modeling languages
- Model-driven engineering languages and systems
- Practical experiences with programming languages
- Program analysis, optimization and verification
- Program generation and transformation
- Programming paradigms (aspect-oriented, functional, logic, object-oriented, etc.)
- Programming tools and environments
- Proof theory for programs
- Specification languages
- Type systems
- Virtual machines and just-in-time compilation
- Visual programming languages

BEST PAPER AWARD

To celebrate WAPL's 10 years old, the 1st edition was in 2007, a Best Paper award will be offered to distinguish a work of high quality presented in the workshop. Award comprises a certificate for the authors and will be announced during the conference dinner.

KEYNOTE SPEAKERS

- Marjan Mernik from University of Maribor (Slovenia) and University of Alabama at Birmingham (USA)
- Jan Vitek from the Programming Research Laboratory, CCIS at Northeastern University, Boston (USA)

STEERING COMMITTEE

- Janousek, Jan, Czech Technical University, Czech Republic
- Luković, Ivan, University of Novi Sad, Serbia
- Mernik, Marjan, University of Maribor, Slovenia
- Slivnik, Božar, University of Ljubljana, Slovenia

SECTION EDITORS

- Rangel Henriques, Pedro, Universidade do Minho, Portugal

REVIEWERS

- Barisic, Ankica, Universidade Nova de Lisboa, Portugal
- Horvath, Zoltan, Eotvos Lorand University, Hungary
- Janousek, Jan, Czech Technical University, Czech Republic
- Kardaş, Geylani, Ege University International Computer Institute, Turkey
- Kern, Heiko, University of Leipzig, Germany
- Kollár, Ján, Technical University of Kosice, Slovakia
- Kosar, Tomaž, University of Maribor, Slovenia
- Lopes Gançarski, Alda, TELECOM SudParis, Evry, France
- Luković, Ivan, University of Novi Sad, Serbia
- Mandreoli, Federica, University of Modena, Italy
- Martínez López, Pablo E. "Fidel", Universidad Nacional de Quilmes, Argentina
- Mernik, Marjan, University of Maribor, Slovenia
- Milašinović, Boris, University of Zagreb Faculty of Electrical Engineering and Computing, Croatia
- Milewicz, Reed, University of Alabama at Birmingham, United States

- **Moessenboeck, Hanspeter**, Johannes Kepler Universitat Linz, Austria
- **Pai, Rekha**, National Institute of Technology Calicut, India
- **Papaspyrou, Nikolaos**, National Technical University of Athens, Greece
- **Porubän, Jaroslav**, Technical University of Kosice, Slovakia
- **Saraiva, João**, Universidade do Minho, Portugal
- **Sierra Rodríguez, José Luis**, Universidad Complutense de Madrid, Spain
- **Slivnik, Boštjan**, University of Ljubljana, Slovenia
- **Splawski, Zdzislaw**, Wroclaw University of Science and Technology, Poland
- **Van Wyk, Eric**, University of Minnesota, United States
- **Varanda Pereira, Maria João**, Instituto Politecnico de Braganca, Portugal
- **Watson, Bruce**, Stellenbosch University, South Africa

Welltype: Language elements for multiparadigm programming

Áron Baráth

Eötvös Loránd University
H-1117 Budapest, Hungary
Email: baratharon@caesar.elte.hu

Zoltán Porkoláb

Eötvös Loránd University
H-1117 Budapest, Hungary
Email: gsd@caesar.elte.hu

Abstract—Modern programming languages try to provide a balance between flexibility to support rapid development and implementing as much validation on the program as possible to avoid expensive runtime errors. This trade-off is reflected in the language syntax, the type system and even in the method how the program produces the runtime binary. While the balance seems to be slightly moved today from safety to effectiveness, there is still a high demand for thoroughly checked, safe, but still effective programming languages. In this paper we introduce our experimental, imperative programming language, Welltype, which is designed to demonstrate that effective development can be accommodated with increased safety. Our language design decisions are based on current real-life problems and their solutions. We describe key features such as syntax improvement, fail-safe type system, and binary compatibility via dynamic linking.

I. INTRODUCTION

MODERN programming languages are not just about higher abstraction level unlike old languages, but aimed to be safer by giving numerous validations. Language evolution is directing toward safer languages. Obviously, a safer language requires more resources to compile in general, but a lot of time can be spared during development as the strong and strict type system saves the programmers from many semantic issues. Nowadays the compilers are fast enough, and most of the programmers will not perceive the overhead of the extra work. However, the user will experience the benefits of a stricter language, because less runtime checks are necessary.

In this paper we present the important features of our experimental programming language, Welltype. This language is aimed to prove that clear syntax, strict semantics and strong type system can still provide a friendly language interface for the programmer.

The clear syntax will help the programmers to understand the code after the development. Benefits during maintenance is guaranteed this way in contrast of a language with a more exotic syntax. A tense syntax can easily overwhelm the understanding of the code.

The strict semantics declares that a construction will mean the same regardless of the syntax context. In practice, when a construction indicates multiple but different things, the intention of the code fragment will be ambiguous. Also, it costs some time to a third person to solve the ambiguity. The *strict semantics* appellation is the bridge between the clear

syntax and the strong type system: since the types are explicit in the code, and a construction means only one thing, the intention behind a specific code fragment is certain.

The strong type system that Welltype uses is much less permissive than the type system in C or C++. We present the type system in Section IV. The key feature is deeply validated types across dynamic linking.

The Welltype language is designed to be as safe as possible with comfortable language features as described above. We made our design decisions based on current and relevant issues in order to fix them with minimal syntactical and semantical overhead. We present details about the key elements and we make conclusions on each of them.

The paper is organized as follows: In Section II we present the Welltype language, and we give a short overview of the key language features. In each of the following 3 sections we focus on one significant language element as an example. In Section III we concentrate on language syntax. Section IV argues for our design decisions on the type system. In Section V we give a short introduction to the binary compatibility and we show how Welltype handles it. In Section VI we show the related work on language safety. Our paper concludes in Section VII.

II. OVERVIEW OF WELLTYPE

The Welltype language is an imperative programming language extended with generic and functional programming elements. It is designed to be safe and feature rich in the same time. The syntax is similar to the C++ with improvements. The structure of the source file is redesigned to meet the *safe* requirement. A Welltype source consists of blocks and metadata directives. A block can be *declaration*, *import*, *export*, or *function definition* block. The first three contain declarations, for example functions, operators, records, enums, algebraic data types, exceptions. Note that the imported/exported declarations will be deeply validated (the mechanism behind is discussed in Section V) during the program loading.

The body of a function can contain assignment statements, assertion statements (which can be turned off in release build), `return` statements, `raise` statements (to raise exceptions), conditional statements (`if-elif-else`), loops (`for`, `while`, `do-while`, `foreach`), and `switch` on algebraic data types and enumeration types (`switch-case`). The complete

grammar is available on the Welltype website [21]. Note that an assignment is not an expression. Furthermore, the semantics disallows free expressions in the code. This improvement (which is clearly a restriction as well) can prevent serious problems on the code snippet that can be seen on Figure 1. The original code was a correct function call, but somehow, the `some_function` identifier is lost from the source code, and the remained statement is still a valid C++ code, but its meaning is totally different. Welltype does not allow the second construction, so the lost `some_function` identifier will cause a compilation error.

```
// original code: function call
some_function(param1, param2);

// errorneous code: sequence operator
(param1, param2);
```

Fig. 1. Error caused by lost function name.

Welltype functions can have exception handler clauses. This syntax decision aimed to keep the source of the function as tidy as possible. Languages like C++ and Java allows to place exception handlers almost anywhere. The problem with this is that the ordinary execution flow will interweave with exception handler fragments that are usually not executed. It can mislead the programmer, and increase the complexity.

In the perspective of the execution, the `raise` statement –and also other sources of exceptions– will find the first exception handler clause on the call stack, and rewind it until the exception handler, and continues. The `raise` statement is very similar to `throw` in C++, but in Welltype programs cannot `throw` exception but they can `raise` them.

For instance, an `IndexOutOfRangeException` will be raised when a `string` or a `seq` is misindexed.

The essential part of the Welltype language is its strong type system. The type system does no support implicit casts, thus the data flow is more followable, and provides faster function lookup. Other restrictions are also encoded into the type system, for example the *mutable* property of a value (variable, or derived value). The Welltype language takes mutable and immutable properties seriously, and in contrast of C++ the *mutable* types should be explicitly tagged – while in C++ the *immutable* (`const`) types should be tagged. We made analysis on some software to determine the ratio of the mutable and immutable function parameters [19]. As an example results on TinyXML [18] can be seen on Figure 2. We concluded that two important reasons support the *mutable*-style instead of the *const*-style. First, much less keywords are necessary; second, if a *mutable* keyword is missing it will cause compilation error at the right place.

An interesting phenomenon can be perceived when we compare the *const*-style and the *mutable*-style approaches. In the *const* world, if the programmer forgets to qualify the function parameter, it will be mutable by default, thus modification may occur. To preserve the parameter (especially

Parameters	236
By value	87
Constant	105
Mutable	44

Fig. 2. Function parameter analysis of TinyXML.

object parameters) from modifications, the programmer must explicitly indicate the intention. In the *mutable*, if the programmer forget to qualify the function parameter and the function wants to modify the parameter, the compiler will emit an error message due to it is forbidden. To allow modifications of a parameter, the programmer must explicitly indicate it. The Welltype follows the immutable-by-default rule when introducing function parameters. This looks to be a larger effort to write the code, but as we have seen earlier, the number of mutable function parameters is the fragment of the number of constant parameters.

III. SYNTAX

Syntax is always a main matter of safety. Syntax defines the face of the language, helps the programmer if it is intuitive, and gives a support to detect general programming errors.

In C [15] and C++ [16], the syntax is quite permissive. Companies define coding conventions (e.g. Apple¹, Google²) that they know (or they think) as good. Some coding conventions can be assumed as broken, or in other words not good enough. For example, a vulnerability called *goto fail* [20], raised because of a duplicated `goto fail` line as can be seen on Figure 3. This vulnerability could be avoidable if the coding rules were adequate.

```
if ((err = SSLHashSHA1.update(&hashCtx,
&signedParams)) != 0)
    goto fail;
    goto fail; // duplicated line here
if ((err = SSLHashSHA1.final(&hashCtx,
&hashOut)) != 0)
```

Fig. 3. The affected lines of the *goto fail* error.

Making the braces mandatory in control flow statements (i.e. `if`) in the language itself is a good alternative. It will guarantee much safer constructions (*goto fail* error cannot happen), and makes the code more readable. The Go language [9] always requires braces in all constructions. The Welltype language follows that design decision, but the position of the braces are different. The detailed specification how to place braces is in the Go language specification [10].

¹[https://developer.apple.com/library-
/ios/documentation/General/Conceptual-
/DevPedia-CocoaCore/CodingConventions.html](https://developer.apple.com/library-
/ios/documentation/General/Conceptual-
/DevPedia-CocoaCore/CodingConventions.html)

²<https://google.github.io/styleguide/cppguide.html>

The WordPress³ team changed their PHP coding standard⁴ to always require braces in 2013⁵, because they saw its benefit. Furthermore, their JavaScript coding standard⁶ also requires braces. Many other relevant discussion can be found about the braces, and where to place them. One thread called *Should curly braces appear on their own line?*⁷ from *stackexchange.com* has numerous of interesting comments. Nowadays, it is not difficult to find coding standard that enforce the usage of braces; even larger communities using them for obvious reasons. Our motivation was the fact it is in coding standards indeed, but the compiler will not complain when it is omitted: better build into the syntax. Requiring something in the coding standard is one thing, but enforcing them to happen is another. Programmers will invest less effort if the code started to work.

Another perspective is to remove all braces (and other symbols and keywords that can introduce blocks) from the language, like the popular Python [12] language. Python is whitespace sensitive, and the blocks will be automatically recognized from the indentation. On the other hand, relying only on whitespaces is not necessarily the safest way. We could separate the elements helping the programmer and the elements helping the compiler. In C, C++, Java, PHP, etc and in Welltype, the indentation is for the programmer to be able to read the code – but the braces are for the compiler, because those will clearly define the block. In a whitespace-only language a misindented statement can cause serious bugs, furthermore, the usually invisible spaces and tabs can also break the “good” indentation, if they are used mixed. And then, no one will know the original intention.

```
if(some_condition); {
    do_something();
}
```

Fig. 4. Erroneous *if* statement (extra semicolon breaks the code).

Still, requiring the braces on the language level can prevent other errors as well, not only the *goto fail*-like errors. The code snippet on Figure 4 is an erroneous code (in C, C++, Java, C#). The extra semicolon after the *if*'s closing parenthesis will close the statement, and the block in the next line is just a regular block. That block has no relation to the *if* statement, but it looks like it has. Since in Welltype a block statement is required as the body of the *if*, the *for*, the *while*, the *do-while* and the *foreach* statement, this kind of error is not possible – that code will not compile. We experienced

³<https://wordpress.org/>

⁴<https://make.wordpress.org/core/handbook/best-practices/coding-standards/php/>

⁵<https://make.wordpress.org/core/2013/11/13-proposed-coding-standards-change-always-require-braces/>

⁶<https://make.wordpress.org/core/handbook/best-practices/coding-standards/javascript/>

⁷<http://programmers.stackexchange.com/questions/2715/should-curly-braces-appear-on-their-own-line>

this and similar errors as a recurrent problem committed by beginner programmers. In many cases the compiler error message was not helping neither.

We presented some aspects of why is a good idea to force block statement as the body of the control flow statements: a little syntactical overhead against the clarity and safety. We conclude that this effort has more benefits than disadvantages.

IV. SEMANTICS AND TYPE SYSTEM

Semantics and the type system is the next bastion of a programming language. Many validations will guarantee that the source fit to the language semantics. Most of these are performed by the type system by checking the types. We consider that the type system is an essential part of a programming language.

One manifestation is to guarantee *const correctness*. The information that a value is mutable or not can improve the code quality, and helps to avoid illegal modifications (e.g. on a read-only memory area). For instance, C++ supports this, but the Java language has really limited support for this. Furthermore, it is hard to force the programmer to write const-correct code [4]. Furthermore, the lambda expressions (that were introduced in C++11) are immutable by default [5] – but that can be modified using the `mutable` lambda declarator [16].

The `mutable` attribute is inherited by the member recursively as it is expected – as well as the `immutable` attribute. Like all attributes `mutable` is part of the type system, therefore it will be stored in the binary. It implies that the `mutable` attribute will be validated during the dynamic linking process, and this guarantees *const-correctness* across binaries.

The type system can be permissive itself that can lead to serious problems – we highlight here only one of them. A synthetic version of the problem can be seen on Figure 5. The snippet is a valid code in several languages (Java, C++, and C#) and it is broken in all of them.

```
// Valid code in Java, C++, and C#
for(char ch='\0';ch<70000;++ch)
{ /* ... */ }
```

Fig. 5. Infinite loop caused by implicit cast.

This construction is a really nasty one, and the programmer may get a warning message for that. Problem is with the loop condition: it compares a `char` and an `int`. Many languages will promote (or cast) the `char` to `int`, because if they do, the comparison makes sense. But the domain of the two types are different, and the left-hand side will never has a value of 70000. Therefore, the loop is an infinite loop. In many languages we just cannot avoid this kind of error. However, in C++ we developed a working solution for this problem [11]. It is a subsequent milestone of our endeavor to make languages safer [19]. Welltype solves this problem only with its strong type system: the comparison `ch<70000` is illegal, due to `char` and `int` cannot be compared.

The Welltype language guarantees that all literals have one, and exactly one type. For instance, the type of the the literal

1u will be `uint`. In C and C++ the literals can have different type depending on the length of the literal. As can be seen in Figure 6 the type of the literal can be different regardless of the suffix. Thus, `sizeof(3000000000)` is not equal to `sizeof(3000000000u)`. In Welltype, the literals that overflow from the domain of its type will cause compile error.

Signed	Type	Unsigned	Type
1	int	1u	unsigned int
2000000000	int	2000000000u	unsigned int
3000000000	long	3000000000u	unsigned int
30000000000	long	30000000000u	unsigned long

Fig. 6. Type of literals in C++ (compiled with g++ LP64 on 64-bit system).

As mentioned earlier, literals in Welltype have exactly one type. The type can be determined in a deterministic way using only the source code itself without its context. That is, if we look at only a single literal, we know its type certainly. For instance, the literal `1234` has the type `int`; the literal `250ub` has the type `ubyte`. A quick overview can be seen in Figure 7. Note that in Welltype a number literal may have underscore (`_`) in it, and it will not change the value of the literal. Underscores will be removed automatically from the literals before further processing. However, the literal `270ub` – in contrast of C/C++ – is illegal, and causes a compilation error. Take the `5000000000u` literal in C; this suggests that it is an `unsigned int` after the suffix, but the literal overflows the `unsigned int` types, and became an `unsigned long`.

Literal	Type
10	int
20_l	long
30_u	uint
40_ul	ulong
50_ib	byte
60_ub	ubyte
70_h	short
80_uh	ushort

Fig. 7. Quick overview of integer literal suffixes.

Since Welltype forbids implicit conversion, problems like on Figure 5 are not possible. We conclude that handling type correctly will decrease the erroneousousness of the code. Additionally, we earlier presented a technique for C++ to avoid implicit conversions [11].

V. LINKING (BINARY COMPATIBILITY)

We talk about binary compatibility when we have multiple releases of a software module. Suppose that we can successfully compile all versions. The question is whether the client binary that uses one of the compiled versions is able to use the other binary versions without modification? When the answer is *yes*, we can say the versions are binary compatible. When we compile and link multiple modules to – for example – an executable we can fix the problem easily: just

recompile the affected modules. However, when we have no control on compilation and linking, like in case of C and C++ dynamic libraries, it is not trivial to decide which versions of the library are compatible. This is a common situation when library maintainers should modify a library and produce a shared object which will be used on-demand by unknown users. Breaking binary compatibility in this case causes the client program to crash. However, the problem is not limited to C or C++, this is a real-life issue, for example, in Java as well [2], [6].

Binary incompatibility can happen in more mystical reasons too. In one of our projects (it was the Welltype compiler itself) there was multiple C++ sources that used the `FlexLexer.h`, which is a system-wide header belongs to the `flex` tool. The source files have been already compiled, when a system upgrade was performed. The `flex` package was upgraded as well, and the `FlexLexer.h` was changed (two fields lost the reference qualifier). After that, one of the source files that use the `FlexLexer.h` changed, and a build was performed. Since the system-wide headers are not a real dependencies in the build system, only the changed C++ files were recompiled – then the executable was linked. Thus the executable crashed, because the changes of the `FlexLexer.h` was not applied in all source, and the old object files became incompatible with the new ones. The problem originated to the linker, because it cannot recognized such inconsistencies.

The Welltype language aimed to avoid binary incompatibilities: since the Welltype dynamic loader **deeply validates** all imported elements, it is able to detect incompatibilities. The signature of the functions are validated, including the name of the functions, number and type of the arguments and the returned types, and the `pure` property. Records are also deeply validated, which consists of name of the record, and number, type and name of the fields. The reason why the Welltype validates so deep, is to detect the changes. For instance, if two fields in a record are swapped, the client program will still contain code for the original record, but the other side assumes the modified version of the record – thus, the program will not work. Therefore, it is reasonable to detect this kind of changes at load time, and the runtime environment can refuse to load the incompatible program.

This mechanism ensures that binary incompatibilities caused by a side effect of the language will not occur, since the binary interface is well-defined. For example, in C++ if the programmer uses only the public API of a class, the compiler may generate inline code that will percolate code from the library into the client program. This is an easy way to make the client program binary incompatible to the next version of the library. However, Welltype prevents this situation, and the binary interface cannot be bridged like in C++.

VI. RELATED WORK

Our research included improving and extending existing mainstream languages. We extended the type system in C++ [11], to forbid implicit casts.

We researched how to check the correct usage of the move semantics in C++11 [1]: the move operation is introduced to improve efficiency, but unwanted copy operations may hidden inside. This area related to the detect heavy runtime overheads at compilation time. We developed a prototype tool (based on Clang Tooling [17], [8]), that can identify when the copy-semantics is used instead of move-semantics, and it is not reasonable. Therefore, the unnecessary copy operations can be eliminated from the code.

We developed an other C++ extension to do compile-time unit testing [7]. This work was inspired by the motto *do as many work at compile-time as possible*. Furthermore, when the unit tests are performed at compilation time, the code is guaranteed as tested, so it is not "too bad"; also, after changed the code will compile again, if it passes the tests, and it cannot be omitted.

The idea to introduce a much restricted type system is not rare. The Scala language also uses a more complex type system with immutable types to increase security [14]. The Rust language represent an other approach to increase security by being resource-safe [13]. Also, this attitude evolving in C++ by the *C++ Core Guidelines* [3]. When a language supports more safety feature, the costs of static analysis will be lower. For example, the C++ language is permissive enough to grow static analysis into a very complex task (CppCheck, Lint, Clang Static Analyzer) – static analysing tools aimed to improve code quality. It would be great if the compiler could perform such task during the compilation.

VII. CONCLUSION

In this paper we presented our experimental programming language, Welltype. As are earlier researches discovered many critical issues in modern programming languages supposed to be safe, we decided to create a prototype language to show that there is a feasible trade-off between safety and the ease of use. We presented revealing examples on three major parts of Welltype: rigorous syntax, strict type system, advanced linking features.

Welltype provides strict syntactical rules to minimize errors caused by typos. Missing or duplicated semicolons, braces or identifiers cause syntax error. The strict syntax also helps code comprehension.

Welltype semantics supposes all function parameters immutable. Measurements on projects implemented in mainstream languages prove that function parameters are mostly supposed not to modify, but mainstream languages do not support this. They threat parameters mutable by default, and may can be changed to immutable only by additional effort. Implicit conversions are other source of runtime errors. Such situations are hard to avoid and even harder to investigate. Welltype's strict type system avoids this kind of problems. By this approach increases safety it has also a positive effect on compilation time as implicit conversions are significant source increased compile time.

Binary compatibility is an issue poorly recognized by language designers, but can cause serious headache for maintainers of large software projects. When already compiled clients are linked against different versions of libraries, incompatible library versions can cause the client code to crash or even worse, to running in undefined way. This problem frequently occurs with C/C++ programs using dynamic libraries, but the issue is not limited to C++, also happens in Java and other languages. Welltype deeply validates modules to link and forbids incompatible usage.

The Welltype compiler is freely available and testable [21]. The language serves as a working prototype to show how safety in various dimensions can extend modern programming languages.

REFERENCES

- [1] Baráth, Á., Porkoláb, Z.: *Automatic Checking of the Usage of the C++ 11 Move Semantics*. ACTA CYBERNETICA-SZEGED 22: pp. 5–20. (2015)
- [2] Dietrich, J., Jezek, K., Brada, P.: *Broken promises: An empirical study into evolution problems in java programs caused by library upgrades*. Software Maintenance, Reengineering and Reverse Engineering (CSMR-WCRE), 2014 Software Evolution Week-IIEEE Conference on. IEEE, (2014), <https://doi.org/10.1109/CSMR-WCRE.2014.6747226>
- [3] Stroustrup, B.: *C++ Core Guidelines* <https://github.com/isocpp/CppCoreGuidelines>
- [4] Cline, M. P., Lomow, G. and Girou, M.: *C++ FAQs*. Pearson Education (1998)
- [5] Järvi, J., Freeman, J.: *C++ lambda expressions and closures*. Science of Computer Programming 75.9 (2010): 762-772. <https://doi.org/10.1016/j.scico.2009.04.003>
- [6] Savga, I., Rudolf M., Goetz, S.: *Comeback!: a refactoring-based tool for binary-compatible framework upgrade*. Companion of the 30th international conference on Software engineering. ACM, (2008), <https://doi.org/10.1145/1370175.1370198>
- [7] Baráth, Á., Porkoláb, Z.: *Compile-time Unit Testing*. 4th Workshop on Software Quality Analysis, Monitoring, Improvement, and Applications pp. 1–7. ISBN 978-961-248-485-9 (2015)
- [8] Duffy, Edward B., Brian A. Malloy, and Stephen Schaub. *Exploiting the Clang AST for analysis of C++ applications*. Proceedings of the 52nd Annual ACM Southeast Conference. 2014.
- [9] Alan A. A. Donovan, Brian W. Kernighan. *The Go Programming Language*. Addison-Wesley Professional, ISBN: 978-0134190440 (2015)
- [10] Go Programming Language Specification. <https://golang.org/ref/spec>
- [11] Baráth, Á., Porkoláb, Z.: *Life without implicit casts: safe type system in C++*. Proceedings of the 7th Balkan Conference on Informatics, ISBN 978-1-4503-3335-1 (2015), <https://doi.org/10.1145/2801081.2801114>
- [12] Summerfield, M.: *Programming in Python 3: a complete introduction to the Python language*. Addison-Wesley Professional, ISBN 978-0321680563 (2010)
- [13] Matsakis, Nicholas D., and Felix S. Klock II.: *The rust language*. ACM SIGAda Ada Letters. Vol. 34. No. 3. ACM, (2014) <http://doi.org/10.1145/2692956.2663188>
- [14] Layka, V., and Pollak, D.: *Scala Type System*. In Beginning Scala (pp. 133-151). Apress. (2015)
- [15] Kernighan, B. W., and Ritchie, D. M.: *The C programming language*. Vol. 2. Englewood Cliffs: prentice-Hall (1988)
- [16] Stroustrup, B. *The C++ Programming Language, 4th Edition*. Addison-Wesley (2013)
- [17] Klimek, M.: *The Clang AST – a Tutorial*. <http://llvm.org/~devmtg/2013-04/klimek-slides.pdf> (2013)
- [18] TinyXML. <http://www.grinninglizard.com/tinyxml2>
- [19] Baráth, Á., Porkoláb, Z.: *Towards Safer Programming Language Constructs*. Studia Univ. Babeş-Bolyai Ser. Inf. LX:(1) 19-34 (2015)
- [20] Vulnerability Summary for CVE-2014-1266. <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-1266>.
- [21] Welltype web page. <http://baratharon.web.elte.hu/~welltype/>

International Conference on Innovative Network Systems and Applications

MODERN network systems encompass a wide range of solutions and technologies, including wireless and wired networks, network systems, services and applications. This results in numerous active research areas oriented towards various technical, scientific and social aspects of network systems and applications. The primary objective of Innovative Network Systems and Applications (iNetSApp) conference is to group network-related events and promote synergy between different fields of network-related research. To stimulate the cooperation between commercial research community and academia, the conference is co-organised by Research and Development Centre Orange Labs Poland and leading universities from Poland, Slovak Republic and United Arab Emirates.

The conference continues the experience of Frontiers in Network Applications and Network Systems (FINANS), International Conference on Wireless Sensor Networks (WSN), and International Symposium on Web Services (WSS). As in

the previous years, not only research papers, but also papers summarising the development of innovative network systems and applications are welcome.

iNetSApp currently consists of tracks:

- CAP-NGNCS'17—1st International Workshop on Communications Architectures and Protocols for the New Generation of Networks and Computing Systems
- INSERT'17 - 1st International Conference on Security, Privacy, and Trust
- IoT-ECAW'17—1st Workshop on Internet of Things—Enablers, Challenges and Applications
- SoFast-WS'17—6th International Symposium on Frontiers in Network Applications, Network Systems and Web Services
- WSN'17 - 6th International Conference on Wireless Sensor Networks

1st International Conference on Security, Privacy, and Trust

ADMITTEDLY, information security works as a backbone for protecting both user data and electronic transactions. Protecting communications and data infrastructures of an increasingly inter-connected world have become vital nowadays. Security has emerged as an important scientific discipline whose many multifaceted complexities deserve the attention and synergy of the computer science, engineering, and information systems communities. Information security has some well-founded technical research directions which encompass access level (user authentication and authorization), protocol security, software security, and data cryptography. Moreover, some other emerging topics related to organizational security aspects have appeared beyond the long-standing research directions.

The 1st International Conference on Security, Privacy, and Trust (INSERT'17) focuses on the diversity of the information security developments and deployments in order to highlight the most recent challenges and report the most recent researches. The conference is an umbrella for all information security technical aspects, user privacy techniques, and trust. In addition, it goes beyond the technicalities and covers some emerging topics like social and organizational security research directions. INSERT'17 is intended to attract researchers and practitioners from academia and industry, and provides an international discussion forum in order to share their experiences and their ideas concerning emerging aspects in information security met in different application domains. This opens doors for highlighting unknown research directions and tackling modern research challenges. The objectives of the INSERT'17 can be summarized as follows:

- To review and conclude researches in information security and other security domains, focused on the protection of different kinds of assets and processes, and to identify approaches that may be useful in the application domains of information security
- To find synergy between different approaches, allowing elaborating integrated security solutions, e.g. integrate different risk-based management system.
- To exchange security-related knowledge and experience between experts to improve existing methods and tools and adopt them to new application areas

TOPICS

Topics of interest include but are not limited to:

- Biometric technologies
- Human factor in security
- Cryptography and cryptanalysis

- Critical infrastructure protection
- Hardware-oriented information security
- Social theories in information security
- Organization- related information security
- Pedagogical approaches for information security
- Social engineering and human aspects in security
- Individuals identification and privacy protection methods
- Information security and business continuity management
- Decision support systems for information security
- Digital right management and data protection
- Cyber and physical security infrastructures
- Risk assessment and risk management
- Tools supporting security management and development
- Trust in emerging technologies and applications
- Ethical trends in user privacy and trust
- Digital forensics and crime science
- Security knowledge management
- Privacy Enhancing Technologies
- Misuse and intrusion detection
- Data hide and watermarking
- Cloud and big data security
- Computer network security
- Security and safety
- Assurance methods
- Security statistics

SECTION EDITORS

- **Awad, Ali Ismail**, Luleå University of Technology, Sweden
- **Bialas, Andrzej**, Institute of Innovative Technologies EMAG, Poland

REVIEWERS

- **Banach, Richard**, University of Manchester, United Kingdom
- **Bun, Rostyslav**, Lviv Polytechnic National University, Ukraine
- **Clarke, Nathan**, Plymouth University, United Kingdom
- **Cyra, Lukasz**, DM/OICT/RMS (UN)
- **Dworzecki, Jacek**, Police Academy in Szczytno
- **Furnell, Steven**, Plymouth University, United Kingdom
- **Furtak, Janusz**, Military University of Technology, Poland
- **Geiger, Gebhard**, Technical University of Munich, Faculty of Economics
- **Grzenda, Maciej**, Orange Labs Poland and Warsaw University of Technology, Poland

- **Hämmerli, Bernhard M.**, Hochschule für Technik+Architektur (HTA), Switzerland
- **Hassaballah, M.**, South Valley University, Egypt
- **Kapczynski, Adrian**, Silesian University of Technology, Poland
- **Kosmowski, Kazimierz**, Gdansk University of Technology
- **Krendelew, Sergey**, Novosibirsk State University, JetBrains research, Russia
- **Misztal, Michal**, Military University of Technology, Poland
- **Pańkowska, Małgorzata**, University of Economics in Katowice, Poland
- **Rot, Artur**, Wrocław University of Economics, Poland
- **Soria-Rodriguez, Pedro**, Atos Research & Innovation
- **Stokłosa, Janusz**, WSB University in Poznan, Poland
- **Suski, Zbigniew**, Military University of Technology, Poland
- **Szmit, Maciej**, IBM, Poland
- **Thapa, Devinder**, Luleå University of Technology
- **Wahid, Khan Ferdous**, Airbus, Germany
- **Yen, Neil**, The University of Aizu, Japan
- **Zamojski, Wojciech**, Wrocław University of Technology
- **Zieliński, Zbigniew**, Military University of Technology, Poland

Risk Management in Access Control Policies

Pierrette Annie Evina, Faten Labbene Ayachi, Faouzi Jaidi
Higher School of Communications of Tunis (Sup'com),
University of Carthage, Tunis, Tunisia
Email: {pierrette.evina, faten.labbene, faouzi.jaidi}@supcom.tn

Abstract—The evolution of information systems and their openness to their socio-economic environment has led to new needs in terms of security. At the heart of information systems, Database Management Systems (DBMS) are increasingly exposed to specific intrusion types, including internal threats due to authorized users. In addition, the access control policy (ACP) defined on a database schema is stored at the same location as the data it protects and is thus highly prone to corruption attempts such as non-conformity of the roles or permissions assignment in the policy observation state compared to a reference state, especially in the case of the Role-based access Control (RBAC). We establish a correlation between the detected anomalies and we explore the log files and other audit mechanisms to propose a global and comprehensive risk management formal approach that mainly verifies the recommendations of the ISO 31000:2009 standard.

I. INTRODUCTION

ACCESS Control is a technique used to grant access to any system by users. The authorization to access the system is usually synonymous of the user's authentication at the entry of the system and the attribution of some privileges or credentials to that user.

The access control is constantly evolving and the environment in which it is implemented is increasingly dynamic. For the Discretionary Access Control (DAC) especially designed for commercial applications, the permissions to access resources are granted by the owner of the data. For the Mandatory Access Control (MAC) specially designed for military applications, access to resources is controlled by an operator and therefore; a user does not have control on his own data [3]. Due to the complexity in the use of this two models, many other access control models have been developed. Role Based Access Control (RBAC), the famous one, uses role to group many users according to their function. It offers, compared to others, a high degree of flexibility when implementing access control policies. Many extensions of the RBAC model exist and aim to secure more the information systems.

Since years, the notion of risk and that of risk management have been introduced in the information security field and the risk-aware access control aims is to reduce the con-

sequences occurring from granting access to a specific information for an unauthorized personnel who can misuse it. The risk is characterized by the potential event, the consequences of that event on the achievement of the objectives and the associated likelihood [2]. As far as its activities and tasks are concerned, each system or organization is exposed to risks which can be caused intentionally or not. Thus, the management of users in the access control system should receive a great attention. Also, the rules governing that access control should be consistent with those established for the access control policy at the designing phase or at a given reference moment.

We propose a system that will enable, indifferently, to thwart the threats related to the action of users on data and those inherent to the changes occurring during the evolution of the access control policy. The remainder of the paper comprises the following paragraphs: paragraph II gives the problem statement; paragraph III presents the main objectives; paragraphs IV discusses the related works; paragraph V presents our methodology; paragraph VI presents our proposed framework ; paragraph VII presents the expected results; paragraph VIII concludes the paper.

II. THE PROBLEM STATEMENT

The environment in which access control systems are implemented is dynamic and increasingly requires rapid and instant decision-making. Also, the ever-evolving technological development of information systems in general and that of access control in particular recommends careful consideration of security risks that could lead to malfunctioning of these systems. The exposure of these assets to threats is inherent to the manipulation of data by suspicious users and the management of the access control policy by wicked administrators.

Unlike traditional access control systems whose policies were based on static decisions, new systems must adapt to the dynamic environment in which the technology evolves and enable decisions to be made automatically based on the

needs related to the risk issues. This requires controlling this risk, and even quantifying it.

To carry out this task, many researchers have studied risk in access control by producing various methods of managing it. For the major part, they have been more interested in the risk associated with users actions on manipulated objects or, to a greater extent, they were interested in the risk associated with managing these users and the permissions assigned to them. Visibly, they were considering that the access control policy was reliable and valid. Thus policies are in fact exposed to various threats and the literature provides very little works that address the technical problems derived from the implementation of the access control policy [1].

Operating an access control policy requires a certain degree of compliance with the specifications defined at its design phase or at an initial phase. We propose to explore this aspect by deeply studying the risk of non-conformity of the rules established for the management of access control.

III. OBJECTIVES

The objective of our work is to develop a system capable of detecting and correcting anomalies that occur in the access control policies management cycle, through an assessment and analysis of the risks linked to the evolution of these policies. This system integrates a sub-system that detect all other forms of anomalies related to the interaction between users and the other access control system resources. Our contribution integrates previous approaches and allows to go beyond the phase of detection of the anomalies towards a complete solution of:

- (a) Recovery on anomaly
- (b) Calculation of the impact of critical anomalies coupled with the logging mechanisms underlying the DBMS
- (c) Specification of a learning and expertise approach on anomalies exploration and the discovery of correlations between those anomalies
- (d) Specification of new mitigation approaches with adequate barriers to reduce the exposure of the ACP and data to subsequent attempts at corruption.

The above points will ultimately leads to a global and comprehensive system for detecting and dealing with anomalies that impede the proper functioning of access control systems.

IV. THE STATE-OF-THE ART

The research on risk management in access control can be classified into two main categories: the access-based approaches and the policy management based approaches. For the access based approach authors calculate the risks associated to access requests. Some authors integrate into their model, the trust and/or the context parameters in order to evaluate that risk. The second category of authors evaluate the risk that is related to the access control policy.

None of the authors produces a fine grained risk management that is related to the changes occurring during the evolution of the access control policy.

Authors in [6] provide a solution to overcome the risk related to unauthorized access of users in an access control system. They use the Bell et Lapadula's access control model. This one is made up of security labels on the objects and the clearance on the subject [6]. They evaluate the trustworthiness of a user and the sensitivity of the evaluated object. It is a matter of determining the risk related to unauthorized access of a user on an object/data. To address this risk, the authors evaluate user confidence and the object sensitivity. The risk associated with unauthorized access is thus quantified in order to dynamically control the actions of the users on data.

Authors in [18] proceed as in [6]. The difference is just that while the late decide to allow access only and only if the trustworthiness is more than the clearance, in [18] authors treat the problem of unauthorized access by identifying different cases : they consider the level of the object sensitivity score compared to that of the subject trustworthiness score and vice versa. Then, a decision is taken in order to deny or to allow the access to the system. The risk is evaluated according to the threat assessment approach used. But the risk caused by sudden and anticipated threat is not taken into consideration as the trustworthiness of the subject and the sensitivity of the objects are established a priori.

As security problems are much more complex in ubiquitous computing compared with traditional environment, authors in [17] plan to make the access control management more dynamic and precise. They evaluate the action of users or processes on the system and take into account the context parameters. These parameters are also considered as input in the risk assessment process .

Authors in [15] evaluate the risk occurred when managing users and permissions through the Role based access control (RBAC) during the pre-mining phase [15]. They consider the constant modification due to the users or permissions creation, modification, or deletion in the access control system. The creation, modification or deletion actions are causes of many mistakes and role misuses. Therefore, they establish a ranking of the users and permissions based on the degree of importance of the risk induced for future mitigation.

In [16], the authors provide a solution to avoid unwanted disclosure of information by corrupted users. They consider the risk occurred when a user manage his own data, granting permission to other users and determine the trustworthiness

of users. They also consider the case where access is inappropriately denied to some users by the owner. They exploit and compute the opinion of a user onto another user to evaluate the loss function due to unwanted disclosure of information through an access control system.

J. Ma, K. Adi, M. Mejri, L. Logrippo in [7] and [8] mainly consider the role delegation issue. Indeed, for a user to delegate his rights to another one, there should be among the two users a trusted relationship. The authors extend the access control architecture in which they incorporate the trust based reasoning. In the case of role delegation, and according to the authors, related risk is computed based on the levels of confidence of the delegate. The risk assessment proposed in [7], [8] highlights the notion of the importance of objects associated with that of criticality of actions of users to those objects.

Authors in [9] propose an access control framework to mitigate insider threats with a risk management process which is adaptive. The changes in users behavior are osculated in order to maintain the trust of each at an appreciable level and above a certain threshold. Below that threshold, authors think that the privileges of this kind of users should be removed. For the purpose, they propose an algorithm that reduces exposure of the access control to risk. They also propose a methodology to help the system administrator in managing inference threats due to the changes of the users behavior.

Users queries are risky especially when there is a misapplication of the rules established in the access control policy. Thus, [13] deal with the risk management in the access control policy, notably the RBAC in distributed databases. The users queries are the main elements observed and considered while assessing risk. Thus, in order to allow an early detection and control of probable negative consequences in the system, the authors in [13] handle and define user risks. Those risks include the bad utilization of users credentials. As far as the access control policy evolves, it is exposed to various corruption attempts. There can be abnormal elements like missed, renamed, hidden users or hidden roles. After they slightly evaluate the risk of having such abnormal elements, the authors plan an assessment module that defines a response monitor.

Our contribution is to produce a comprehensive and global system that addresses risk management in access control policies during its evolution. It is necessary to identify the anomalies. Specifically, we study the correlations that may exist between one or more detected anomalies. This will make it easier to interpret the

corruption risks to which the policy of access control is subjected.

V. METHODOLOGY

The intention of the present research started from a previous work. Indeed, anomalies of non compliance of access control policy have been defined. But we believed that there exist a correlation between two or more anomalies and that can lead to other threats. This threats have to be defined.

The first task consist in an analysis of the results of that previous work.

In order to get more information related to our work plan, the second task is the documentary research. An important number of publications have been identified and studied in order to precisely identify our subject. Some publications have enabled us to establish the state-of-the-art.

Another step is the one during which we explore the log files. this will allow us to collect information about recurrent attacks, i.e data that are regularly and improperly exploited, as well as anomalies of non-compliance (or revelations about users, hidden roles, and so one).

A simulation on a real database is done, with real schemes and tables created. This will enable us to verify our results, qualitatively and quantitatively.

We use the Markov chains to model the unauthorized accesses and thus to model the illegal behavior users.

Our expectation is to come out with new concepts that we believe will be adopted and will advance research in the security of information systems, the security of access controls and the security of databases.

VI. OUR PROPOSED FRAMEWORK

Unauthorized update of the access control policy is largely responsible of data corruption. This situation can be exploited by a criminal who wants to access the database. However, at the present stage of research, we could not find an intrusion detection system that can detect this type of anomaly. But, it is possible to trace the action of users on the database. Thus, suspicious and unauthorized users are detected using the log files of the database system. The tracking of these users is therefore the first step in our anomaly identification process, which allows us to identify unauthorized access as well as the recurrent targeted data.

Thereafter a correlation is defined and established between these different anomalies in order to detect the induced faults. Thus, a user who fraudulently accesses a protected data is an usurper who has certainly benefited from the privileges that have been attributed to a role that is not reserved for him.

As a result, the recurrent targeted data is identified and a list of such sensitive data is established. At the end, we draw a resultant architecture which is based on international stan-

dards. Indeed, as recommended by the ISO 31000: 2009 standard, our Risk Management System (RMS) is composed by (i) a Risk Assessment Engine (RAE) and (ii) a Risk Treatment engine (RTE). (figure 1) The risk assessment phase is usually developed in 4 steps: Context assessment, Risk Identification, Risk Analysis and Risk Evaluation [19].

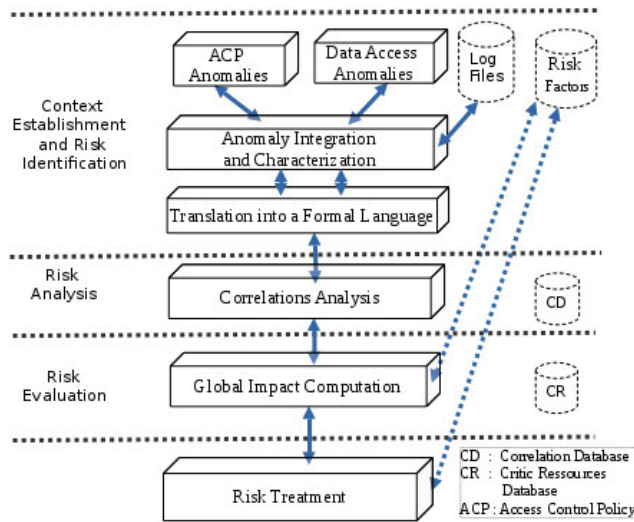


Fig. 1 : A framework for risk management

The risk contextualization concerns the identification of the assets in the database system that are to be protected. It is at this stage that the scope of the risk management is defined as well as the risk criteria to be used later on in the risk management process.

The risk identification concerns the identification of vulnerabilities that threaten data. It consists in computing the set of suspicious users and targeted data. the aim of risk identification is to make a complete list of risk that will be the object of the further steps of the risk assessment process.

The risk analysis that will confirm or deny the corruption of the data and the criticality of the vulnerability as it explores the authorized access scenarios based on data from log and audit security mechanisms activated on the Database Server. This enables to detect and establish the intrusive user behavior and thus, to reinforce the Intrusion Detection Systems (IDS)

The risk evaluation is a phase of self-adaptation that allows our system to correct its estimate of the risk incurred. It uses the results of the analysis phase to adjust the risk factors.

The risk treatment consist mainly in avoiding risk, mitigating it, and removing its source or changing the likelihood of it occurrence as recommend in [1]. A risk treatment plan is usually put in place and shows the procedure. That treatment plan precise the different actions

to be taken, the persons responsible of applying the plan, the resource requirements, the performance measures and constraints, the reporting and monitoring requirements and the timing and schedule.[1]

The concrete process of our risk approach related to our framework is shown in the following (figure 2)

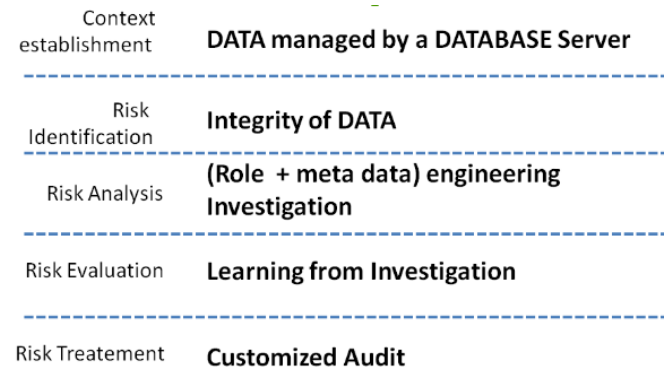


Fig. 2 : The approach process

VII. EXPECTED RESULTS

Before going into details, let us give the list of the main awaited results. This are:

- design of an intrusion detection system for unauthorized update of access control policy
- detection of induced faults by establishing a correlation between the detected anomalies
- list of the recurrent targeted and sensitive data
- detection and establishment of the intrusive user behavior and thus, reinforcement of the Intrusion Detection Systems
- production of a global and comprehensive system for risk management for access control systems

To illustrate this while considering the above framework, we should have a fairly complete list of anomalies and an evaluation of the related risk which is determined with our risk assessment approach.

This has been initiated by a previous work by F. Jaidi and F. Labbene Ayachi in [14]. Indeed, as stated in RBAC standard, ACP is defined as the set of all users, roles, permissions and assignments, i.e $ACP = (USERS, ROLES, PERMS, AUR, ARR, APR)$ where AUR, ARR, APR represent respectively the user-role assignment, the role-role assignment, and the permission-role assignment.

ACP is the formal specification of the policy and ACP' is the formal representation of the implemented policy. ACP contains the elements as specified in the early stage of the policy engineering. Within the framework of the RBAC, these elements ideally reflect the concepts related to the

definition of users, roles and permissions, the allocation of roles to users, the allocation of roles to roles, the assignment of roles.

On the other hand, the elements of the ACP' contain concepts that are also related to the definition of users, roles and permissions, the allocation of roles to users, the allocation of roles to roles, the assignment of roles . This concerns the implementation of the policy by the managers, taking into account the access of malicious users to the data and also taking into account possible accidental corruption of the policy.

Things could be perfect if ACP' was conform to ACP. Unfortunately, this is not always the case. So, to verify that ACP' is conform to ACP, their elements are compared. In [1], this comparison has been done and among others, the following anomalies have been defined :

- hidden users which are visible when new users, not initially defined, are injected in the concrete instance ACP'
- hidden roles are observable when new roles, not initially planned, are introduced in the concrete policy ACP'.
- hidden access flow (HiddenACF) is perceptible in the case of illegal assignments of roles to roles, roles to users or permissions to roles.

To go further in the interpretation of corruption attempts, we consider the correlation between these anomalies, we come out with some new anomalies definitions expressing unauthorized accesses.

Considering the frequency of occurrence of each of these events that constitute an anomaly, random variables are thus defined. A relationships of dependencies can be established between them. Hence, a statistical link can be established between these variables since the increase or decrease of one variable is related to the increase of the other variable.

Concretely, a hidden role implies action. This presupposes permissions, delegations and users that were not considered in the policy as initially defined (these are for example, hidden users, hidden roles, hidden assignments). An analysis of the correlations makes it possible to identify critical anomalies that lead to high risks of corruption of the policy. We thus define, notions such as suspicious users or altered roles. This is done in the following way:

Definition 1: (Suspicious users)

We define in (2) a suspicious user as:

$$\text{SuspiciousUsers} = \{u \in \text{USERS} \mid r \in (\text{HiddenRoles} \cup \text{AlteredRoles}) (u, r) \in \text{AUR}'\}. \quad (1)$$

where USERS is the set of the users of the access control policy.

Definition 1: (Altered Roles)

We define in (1) an altered role as:

$$\text{AlteredRoles} = \{r \in \text{ROLES} \mid r' \in \text{HiddenRoles} (r',r) \in \text{AUR}'\} \cup \{r \in \text{ROLES} \mid p' \in \text{PERMS}' (r, p') \in \text{APR}'\}. \quad (2)$$

where ROLES is the set of roles defined in access control policy and PERMS is the set of permissions to be granted in the access control policy.

We intend to use the Markov chains to model these unauthorized accesses and thus to model the illegal behavior of a user. We try to ameliorate in an incremental manner the model obtained and to attribute a weighting according to the frequency of occurrence of a given unauthorized access. For risk assessment, risk factors will be assessed taking into account the correlation coefficients for those events or anomalies identified.

VIII.CONCLUSION

Information systems, including database systems, are exposed to threats of any kind arising out of the use of malicious users. This is submitting the data to the risk of alteration and destruction. Since the access to these systems are filtered by access control systems, insiders threats are certainly responsible for loss of integrity, confidentiality, data availability. But, the access control policies that regulate these accesses are also source of danger to the information systems as far as their evolution is concerned although they are generally considered valid and reliable. Indeed, from the design phase to the implementation phase, these policies are not always conform to the initial phase or to an intermediate phase taken as reference. Anomalies of non-conformity in the ACP have been the subject of the work of F. Jaidi and F. Labbene Ayachi, who defined some of them.

By studying the correlation between these anomalies and using the log files that are intrinsic to the system, we think we can detect other anomalies whose risk is also evaluated by faithfully applying the recommendations of the international standards, such as the recommendations of ISO 31000. So, We propose a system to detect and mitigate risks for access control policies. This system will take into account other intrusions detection systems (IDS) in order to produce a global and comprehensive system for risk management in access control systems.

REFERENCES

- [1] F. Jaidi and F. Labbene Ayachi. "A Risk Awareness Approach for Monitoring the Compliance of RBAC-based Policies". In Proceedings of the 12th International Conference on Security and Cryptography (SECRYPT-2015), (pp 454-459). DOI: 10.5220/0005577304540459
- [2] International Electrotechnical Commission, International Standard, ISO/IEC 31010:2009, First Edition, 2009.
- [3] R. Sandhu, E. J. Coynek, H. L. Feinsteink, and C. E. Youmank. (1996) "Role-Based Access Control Models", IEEE Computer, vol. 29, no. 2, (pp. 38-47). DOI: 10.1109/2.485845
- [4] K. Z. Bijon , R. Krishnan and R. Sandhu. (2013). "A Framework for Risk-Aware Role Based Access Control". 6th Symposium on Security Analytics and Automation. DOI: 10.1109/CNS.2013.6682761
- [5] International Electrotechnical Commission, International Standard, ISO/IEC 31010:2009, First Edition, 2009.

- [6] P.-C. Cheng, P. Rohatgi, C. Keser, P. A. Karger, G. M. Wagner, A. S. Reninger, (2007). "Fuzzy MLS: An Experiment on Quantified Risk-Adaptive Access Control", In *Security and Privacy*, (pp. 222–230). DOI: 10.1109/SP.2007.21
- [7] J. Ma, (2012). "A formal approach for risk assessment in RBAC systems". *Journal of Universal Computer Science*, vol. 18, pp. 2432-2451. DOI: 10.3217/jucs-018-17-2432.
- [8] J. Ma, K. Adi, M. Mejri, L. Logrippo, (2010). "Risk analysis in access control systems". In *Eighth Annual International Conference on Privacy Security and Trust (PST)*, pp. 160-166. DOI: 10.1109/PST.2010.5593248.
- [9] N. Baracaldo, J. Joshi, (2013). "An adaptive risk management and access control framework to mitigate insider threats", *Computers & Security*. DOI: 10.1016/j.cose.2013.08.001.
- [10] F. Feng, C. Lin, D. Peng, J. Li, (2008). "A trust and context based access control model for distributed systems". In *Proc. of the 10th IEEE International Conference on High Performance Computing and Communications, HPCC '08*, pp. 629-634. DOI: 10.1109/HPCC.2008.37
- [11] L. Chen, J. Crampton, (2011). "Risk-aware role-based access control". In *Proc. of the 7th International Workshop on Security and Trust Management*. DOI : 10.1007/978-3-642-29963-6_11
- [12] A. Bouchahda-Ben Tekaya, N. LeThanh, A. Bouhoula, F. Labbene Ayachi, (2010). "An Access Control model for Web Databases". *24th Annual IFIP WG 11.3 Working Conference on Data and Applications Security; DBsec 287-294*. DOI : 10.1007/978-3-642-13739-6.
- [13] Ebru Celikel, Murat Kantarcioglu, Bhavani Thuraisingham and Elisa Bertino. "A risk management approach to RBAC". *Risk and Decision Analysis 1 (2009) 21–33*. DOI 10.3233/RDA-2008-0002. IOS Press.
- [14] F. Jaidi and F. Labbene Ayachi. (2015). "A formal approach based on verification and validation techniques for enhancing the integrity of concrete role based access control policies". In *International Joint Conference* (pp. 53-64). Springer International Publishing. DOI: 10.1007/978-3-319-19713-5_5.
- [15] Alessandro Colantonio, Roberto Di Pietro, Alberto Ocello, and Nino Vincenzo Verde, "Evaluating the Risk of Adopting RBAC Roles", ara Foresti; Sushil Jajodia. *Data and Applications Security and Privacy XXIV*, 6166, Springer, pp.303-310, 2010. DOI: 10.1016/j.dss.2010.08.022.
- [16] Chris Burnett, Liang Chen, Peter Edwards and Timothy J. Norman, "TRAAC: Trust and Risk Aware Access Control", 2014, Twelfth Annual International Conference on Privacy, Security and Trust (PST). DOI: 10.1109/PST.2014.6890962.
- [17] Nguyen Ngoc Diep, Le Xuan Hung, Yonil Zhung, Sungyoung Lee, Young-Koo Lee, and Heejo Lee. "Enforcing Access Control Using Risk Assessment", *Proceedings of the Fourth European Conference on Universal Multiservice Networks (ECUMN'07) 0-7695-2768-X/07 \$20.00 © 2007*. DOI: 10.1109/ECUMN.2007.19
- [18] Hemanth Khambhammettu, Sofiene Boulares, Kamel Adi, Luigi Logrippo. "A framework for threat assessment in access control systems" that appeared in *Proceedings of 27th IFIP TC 11 Information Security and Privacy Conference (SEC 2012)*, 2012. DOI: 10.1007/978-3-642-30436-1_16
- [19] Pierrette Annie Evina, Faten Labbene Ayachi, Faouzi Jaidi and Adel Bouhoula, "Towards a Reliable Formal Framework for Enhancing Risk Assessment in Access Control Systems", *EPiC Series in Computing Volume 45*, 2017, Pages 77–82 SCSS 2017. The 8th International Symposium on Symbolic Computation in Software Science 2017

Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection

Artur Rot

Wroclaw University of Economics
ul. Komandorska 118/120
53-345 Wroclaw, Poland
Email: artur.rot@ue.wroc.pl

Boguslaw Olszewski

University of Wroclaw
Pl. Uniwersytecki 1
50-137 Wroclaw, Poland
Email: boguslaw.olszewski@uni.wroc.pl

Abstract—According to Kaspersky Lab research, APT – Advanced Persistent Threats – are one of the biggest threats in IT as of 2016. Organised groups, keeping contact in various languages, have attacked the IT systems of financial institutions, government, military and diplomatic agencies, telecom and power supply companies, politicians and activists, and private companies, and these attacks were global in scope. APT should be seen as a complex phenomenon, an existing danger to companies, organisations and public entities. This article showcases the problem of APT, the biggest threats related to them, and chosen methods and tools that can be effectively used to counter APT attacks. An effective, multi-layered defence model is outlined in the article as well.

I. INTRODUCTION

The term “cybersecurity” has become very popular nowadays, and the problems of Internet security and of protecting internal networks of various organisations are discussed widely, not only in everyday life, but also in various business sectors. Despite hundreds of millions of PLN spent by companies annually on cybersecurity, most organisations are constantly under threat of APT, which remain undetected for months and cause tangible losses in company functioning and image [15]. Companies and government institutions are increasingly often the target of APT attacks, difficult to detect and leaving no traces. In 76% of organisations harmed by APT, antivirus software and breach detection systems did not block the attack. Examples of effective attacks on not only international companies, but Polish government agencies as well, show that APT attacks are a new field of battle for the government, commercial companies and criminal organisations. During the *Infosecurity Europe 2011* conference, APT were included among the biggest cyber threats of the modern world, and their character requires a different approach than the one usually in use. According to the Deloitte report *Cyber Espionage – The harsh reality of advanced security threats* [4], the key factors in fighting the newest cyber threats, including APT, are: constant risk evaluation, implementing offensive security means, and training staff to appropriate responses [5] [18]. The subject of cybersecurity suffers, however, from insufficient research and literature, due to its

constantly changing environment and designates – this, in turn, caused by its changing technological, social, military and political aspects. A similar problem can be observed with APT, a phenomenon that is still developing and as such should be considered in more depth. Thus, the authors of this article aim to present the phenomenon of APT and to fill the gaps in subject literature as to the APT dangers for practically any organisation and company, and the methods and means of defence against the attacks. Authors have also presented an effective, multi-layered defence model.

II. APT ATTACKS – A NEW FORM OF CYBER THREATS

APT attacks are a complex, long-term set of actions aimed against specific persons, organisations or companies. They are most often instigated by attackers who study a given company and its staff for months before initiating the attack. They use tools which minimise the chances of detection, and can thus steal data over a long period, perhaps over many months. The APT attacks differ from security breaches hitherto known by exactly that – the difficulty in detection and the wide scope [5].

APTs are defined as a new and more sophisticated version of known multistep attack scenarios and they are targeted specifically to achieve a specific goal, most often espionage [7]. They are “advanced” in that the malware they use is advanced, but also the character of the danger they pose. APTs use complex tools and are aimed to sabotage, steal confidential data, to defraud or blackmail. Hackers causing APTs are not only very well educated, but also have tools and funding necessary for making these threats effective. Their complex methods of introductory research and background checks are not, however, revolutionary and make use of known social engineering. These remain universal, despite a large body of knowledge and counter-strategies. It's the network access and the attack itself that make the persistent threats advanced.

The other distinctive trait of APTs is their Persistence, related to the character of operations. APTs are not incidental, they form a cohesive strategy that aims to fulfil a larger goal. The priority is to remain undetected as long as possible, systematically fulfilling this goal. These goals are

usually financial profits. The threat is mostly related to the human factor, the highly organised groups. They are strongly motivated (by their hierarchy or by financial possibilities), they create command chains and specialised subgroups dealing with specific parts of an APT attack. The APT attackers are usually specialised teams of IT professionals and their clients – usually governments – using advanced technologies and obscure points of attack to obtain sensitive data. APTs are also called directed attacks, since the targets are chosen deliberately and studied beforehand to find the best point of attack.

III. CRUCIAL POINTS OF AN APT LIFE CYCLE

A typical APT life cycle (see Fig. 1) is divided into four stages: reconnaissance, initial compromise, establishing foothold and infiltration. Reconnaissance allows to find effective points of attack, evaluate target susceptibility and the people within the organisation who can, actively or passively, facilitate security breaches. These may be employees without any crucial access credentials, but who can allow for further infiltration of a given system in the long run.

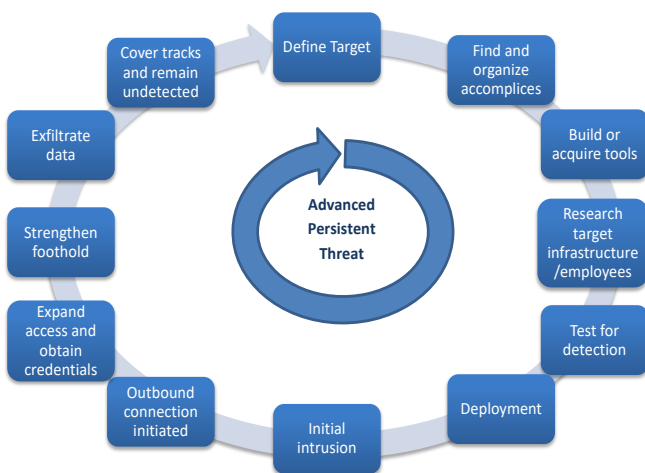


Fig. 1. APT life cycle [20]

The preparation stage allows for the second stage of an APT life cycle. An initial compromise is the result of the attackers gaining access to some element of the internal network: a desktop computer, a network device, a PC, pendrive or smartphone of a specific person who has high credentials, or someone who uses such hardware in their professional or private life. This is facilitated by unauthorised use of private devices within the professional network, and an inclusion thereof into the corporate IT system. Social engineering is important at this stage, as it is at the previous stage: APT attackers usually introduce malware, Trojan horses or apps that allow for further remote actions within the network with help from social engineering.

A negative attempt at detection allows further intrusions and malware introduction, which in turn creates a communication channel for the attackers (Command&Control Server, C&C). The third phase is assuming control over the desired parts of a system and possibly over other users, in order to gain access to whatever data is the main objective. The fourth stage entails a long term infiltration process based on credentials obtained, and later on, escalating access privileges to gain more power and at the same time make the breach less noticeable. Obtaining or destroying the crucial data is initiated - whatever was the objective of the hackers or their clients. When it's done, the attackers retreat and cover their traces, deleting signs of their presence and any data that might allow for identifying the source of the attack.

IV. EXPLOITING VULNERABILITIES

Treating APT as cheap sensationalism or another marketing campaign is underestimating and misrepresenting the phenomenon. Thus, the first source of vulnerability to APT is the human factor, especially the low awareness of APT danger and the techniques used by APT attackers. Lack of this awareness leads employees to behaviour they themselves don't know is irresponsible, both in the workplace and their private life, opening entrance points for an APT attack [17]. Knowledge and awareness on the part of network admins, IT security teams and especially decision-making personnel, who assign funds and implement procedures, is also important.

Social engineering and widely available information about specific employees (blogs, social media, company websites) allow the attackers to pinpoint the individuals with high level credentials, allowing access to strategic data or network resources, or simply individuals who can inform the attackers about the next target on their way towards these credentials, towards their objective and the next APT stage. Knowing an employee's profile, the attackers evaluate their weaknesses and possible means of approaching them, including blackmailing or bribing them into offering their abilities and means to the attackers.

A directional APT means a complex, multi-faceted process aimed at achieving the goals of specific stages. From the social engineering angle, this means spear phishing – an unauthorised access to data, network resources or hardware, through a specific person, including accessing resources belonging to another employee or even organisation. Spear phishing begins right at the reconnaissance stage, and culminates in a personalised phishing attack, wherein the victim receives a personalised email and, convinced about its safety and trustworthy source, opens attachments or clicks provided links.

Social engineering, exploiting personal vulnerability, is one of the most important means of initiating an effective infection of the target network, and is the most popular method of accessing the necessary resources. The second

most effective type of attack is the zero-day attack, exploiting software vulnerabilities. Hackers use them to circumvent classical defences, based on software signatures in antivirus and firewall programs. Numerous vulnerabilities can be also found in hardware, and these are increasingly used with the spread of wireless devices. Hardware vulnerabilities complement software vulnerabilities, especially in microchips, where manufacturers often leave an access point on purpose, to use in post-manufacturing tests [11].

Business organisations and companies are the most popular targets of APT attacks, with education, finance, technology, space exploration and aviation, power supply, chemistry, telecom, medicine and consulting being the most often targeted branches.

V. DEFENCE AGAINST APT ATTACKS

The most successful form of defence against APT is constant monitoring and reaction to as many APT attempts as possible. Identifying an attack attempt through any channel makes that channel obsolete. Strategies of defence based on one or two APT levels are insufficient: as mentioned before, in 76% cases, antivirus software was no obstacle at all to APT attacks [4]. Therefore, first generation security means are not enough to protect valuable targets, and prevention systems do not guarantee protection anymore. Experts confirm that “any effective approach to defending against APTs must include defence in depth, a detection capability, an APT incident response plan, a recovery plan, and security awareness and training” [2].

The basic means of countering APT attacks are a set of basic procedures that limit the relatively simple elements of the APT process. When APT is divided into its basic elements, these usually prove to be well known and easy to counter. It is their combination, especially in a sequence created specifically for a given target, that makes defence against APT difficult. This is why even the best means of network security, including proxy servers, firewalls, VPN and antivirus software cannot defend against an APT on their own. Initial protection methods include implementing a vulnerability management process, system updates and penetration tests. These should be complemented by detailed documentation on influence and risk evaluation. Determining the crucial resources and the elements in need of special protection is vital, especially for business targets.

Pro-active protection allows to eliminate a point of attack right at the preparation phase, excluding it at the planning stage. The more points of attack are blocked, the more time, effort and resources must the APT attackers spend. Protecting vulnerabilities, using antivirus software and blacklisting requires modification and real time protection: in-line bi-directional scanning and behavioural analysis. Among desirable solutions is SSL protocol scanning, allowing for advanced detection of potential intruders. Similarly to APT threats themselves, means of protection

must be long-term and persistent, especially given the rising use of wireless devices, the presence of which within the organisation must be constantly monitored.

Another type of means of protection is detecting an ongoing APT. This entails chiefly the ways of detecting malware already introduced – programs that keep up and speed up an APT attack. The biggest problem with APT malware is the fact that neither antivirus software nor IDS (Intrusion Detection System software) will have its signature in their databases. Attackers use evasion techniques to hide malicious code, which is polymorphic and customised to a given target, or dynamically modified during the attack. Detecting APT will activate the means used to contain and isolate it, and to return to the state from before the attack. This is the third category of APT protection. Its main components are an online analysis (determining the traits of a specific APT), real time reporting and correlated log analysis, for example based on SIEM (see below), in order to recognise and neutralise a threat in the future. The last element is evaluating the entirety of implemented methods.

Two main types of APT defences can be distinguished today: hardware-based and cloud-based [17]. In the first case, a dedicated device is placed on the edge of the protected network, monitoring and informing about suspicious traffic basing on reputation indexes (it does not block transmission in real time). More advanced models perform behavioural analysis and sandboxing.

Hardware-based solutions have certain limits. Despite high costs – which limit their numbers, and restricts use to big companies, especially for models that monitor encrypted traffic – these devices are not able to register the entirety of network traffic, given the rising use of mobile devices and remote workstations. The alternative cloud-based solutions are supposed to eschew most of the limitations of hardware-based solutions. These are supplied as a multi-user platform and offer more effective traffic monitoring, threat intelligence in real time on every APT stage and are scalable. The hardware approach is replaced by holistic analysis (behavioural, vulnerabilities, address filtering, SSL transmission monitoring, active content etc.) Practise shows that mere observing procedures and basic protection is not nearly enough to shield from APT, hence the importance of advanced, multi-layered protection methods described below in the end-to-end strategy.

A. Multi-layered APT Protection Model

Another solution for APT protection is the so-called defence-in-depth. It's a multi-layered strategy that entails careful protection of each layer of the network: the people, the devices and applications. It's complex character significantly increases the chance of successfully resisting an APT attack, since it's based on permanent monitoring of the network and security control.

Defence-in-depth means, therefore, a layered approach to network security, and taking steps to detect a threat, react to

it and eliminate it, in every layer. The seven-layer model based on OSI creates an environment where none of the layers protects against an APT on its own, but their combination is a cohesive barrier. The model also entails physical security means, carried out through protecting the organisation space – protecting facilities where devices are stored, eliminating vulnerabilities caused by nature or by contact with outsiders, etc.

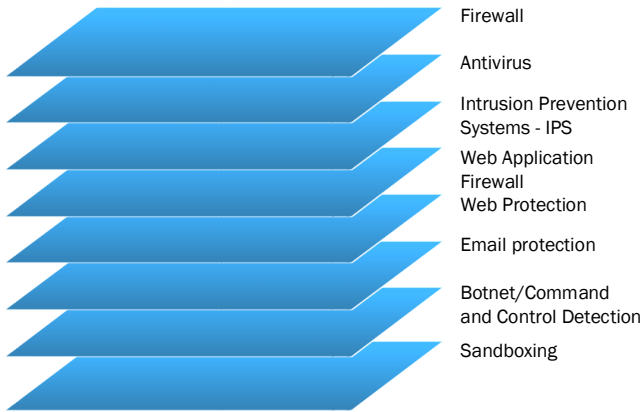


Fig. 2. Layered APT defence model [9]

In the end-to-end strategy presented below (see Fig. 2), a firewall software is the first line of defence against an APT, blocking ports and filtering packets. Next generation firewalls (NGFW) usually combine the typical functions of firewalls (packet filtering, website blocking, virtual IP addresses) with IPS, application control and context protection (e.g. Cisco ASA 5500-X Series). Antivirus software is another layer that limits potential system breaches, since it scans all packets (not just their headlines), as well as compressed and encrypted files.

The next element, an Intrusion Prevention System (IPS), allows for an in-depth monitoring of network traffic and vulnerabilities, especially if equipped with zero-day threat minimising mechanisms. It's a successor of the Intrusion Detection System (IDS), which was based on passive monitoring and danger reporting based on an analysis of network traffic copy, remaining integrated into the data flow and allowing for blocking. The two systems also differ by their functioning: IDS uses exploit signatures, while IPS included detection based on anomaly statistics and vulnerability signatures.

A Web Application Firewall is a transparent system of vulnerable web app protection, which works basing on whitelists and blacklists – a database of permitted and banned elements. This allows to protect the servers working in the demilitarised zone, which most often host organisation websites.

The multi-layered model is complemented by the web protection layer, the email monitoring component, and the sandbox – an isolated test environment, either virtual or supplied by hardware.

B. SIEM Platform as a Form of Defence Against APT Attacks

Another suggested method of APT defence is implementing second generation SIEM tools (Security Information and Event Management) – a platform allowing for managing information relating to security and incidents (see Fig. 3). Monitoring diffused system logs, network devices and applications in real time allows for more effective control over processes and resources, and for intercepting proof of an ongoing APT in the operative risk management phase, basing on compromise indicators. Forensic analysis allows to determine the origin, character and type of a given event on a given device, as well as other components indicating a vulnerability.

SIEM platforms, available on the market since the late nineties, are still in development and currently await upgrades in their report and correlation functions. However, implementing an SIEM system even in its current form is a significant upgrade of an APT defence. SIEM functional components offer “collection and archiving data, detailed event and normalisation analysis, reports, queries, and usually some form of a real-time analysis module” [14]. Until fully developed SIEM tools appear, implementing them in their current state should be an auxiliary measure, and clients should selectively define their priorities and choose the most adequate mechanisms. Data volume is a separate question, requiring the use of terabyte disks or data clouds, and influencing response time. A typical SIEM will process several hundred thousand events per second.

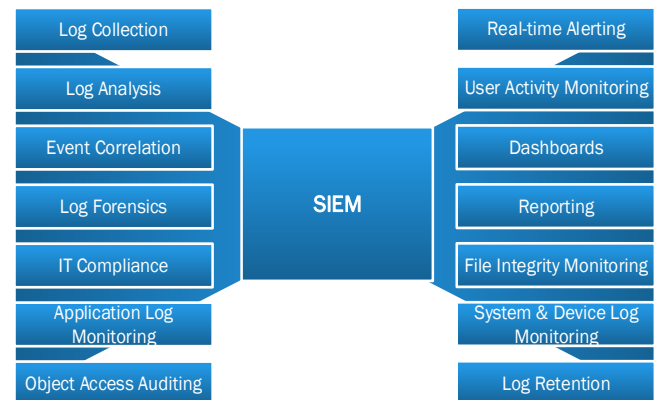


Fig. 3. Security Information and Event Management [21]

Among the most important platforms are, for example, QRadar IBM, Q1 Labs Qradar, and NetIQ Security Manager. These solutions have limits as far as analysing data gathered for months or years is concerned [1], which means that a new generation of APT defence becomes crucial.

C. Big Data Technology in Detecting and Resisting APTs

The third generation tools are technologies of large-scale data management: Big Data, also called second generation SIEM. It allows to analyse large quantities of data and can generate and transmit it quickly, as well as search for

variables and unstructured resources. This means it fits APT protection processes very well. Technologies such as Apache Drill or Dremel allow to analyse streaming data in real time, and therefore propose to use an APT detecting mechanism through an integrated log analysis and anomaly detection based on a typical pattern customised for a given organisation [8], or behavioural analysis based on Big Data. It has been proven that solutions based on MapReduce, Hadoop or Hive allow to shorten the analysis time about twenty times [1]. IBM combines their Qradar SIEM system with a Big Data platform [10], sending data collected even over several years to further analysis in SOC. Zscaler company offers a Zscaler Cloud Sandbox [22]. Big Data technologies are currently one of the most promising ways of APT defence, especially given the rapidly increasing amount of data: in 2013, the Hewlett-Packard network alone generated 12 million events per second [3].

I. CONCLUSION

The above is not an exhaustive presentation of means and technologies of preventing, detecting, and eliminating APTs. The market offer expands dynamically, as do the theoretical foundations of such defensive actions. Among other offers of APT protection are such technologies as deep learning (SignalSense), requiring a new approach to network security, constant monitoring, adaptation and learning through experience [19]. PwC, in its *Global State of Information Security Survey 2015* notes that within organisations, it was the current (31%) or former (27%) employees are the source of insider threats [13]. Therefore, more attention should be paid to monitoring internal traffic, in this particular example, based on Neural Network (scalable detectors, host classification, IP, packets and traffic reputation), which searches for divergences from the usual pattern of network behaviour.

To summarise, strategies for organisations include integrated information exchange between security points, advanced prevention and detection, including a broad strategic approach (tactical hardware configuration and attack scenarios), SSL traffic monitoring and ensuring full protection.

REFERENCES

- [1] *A Case Study In Security Big Data Analysis*, 2016, <http://www.darkreading.com/analytics/security-monitoring/a-case-study-in-security-big-data-analysis/d/d-id/1137299>
- [2] Ashford W., "How to combat advanced persistent threats: APT strategies to protect your organization", 2016, <http://www.computerweekly.com/feature/How-to-combat-advanced-persistent-threats-APT-strategies-to-protect-your-organisation>
- [3] Cárdenas A.A., Manadhata P.K., Rajan S. (eds.), *Big Data Analytics for Security Intelligence*, Cloud Security Alliance, 2013, https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Analytics_for_Security_Intelligence.pdf
- [4] *Cyber Espionage: The harsh reality of advanced security threats*, Deloitte: Center for Security & Privacy Solutions, 2016, https://www.isaca.org/chapters1/phenix/events/Documents/cyber_espionage.pdf
- [5] Gajewski, M., „Cyberataki typu APT nowym frontem wojny”, Chip.pl, 2013, <http://www.chip.pl/news/bezpieczenstwo/luki-bezpieczenstwa/2013/03/cyberataki-typu-apt-nowym-frontem-wojny>
- [6] *Cyberbezpieczenstwo 2016: 5 trendow, jakich powinnismy sie obawiac*, <http://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/914855,cyberbezpieczenstwo-2016-5-trendow-jakich-powinnismy-sie-obawiac.html>
- [7] Ghafir I., Prenosil V., "Advanced Persistent Threat Attack Detection: An Overview", *Proceedings of International Conference On Advances in Computing, Electronics and Electrical Technology*, Kuala Lumpur, 2014 p. 154
- [8] Kim H., Kim J., Kim I., Chung T., "Behavior-based anomaly detection on Big Data", *The Proceedings of the 13th Australian Information Security Management Conference 2015*, Perth, 2015, pp. 73-80
- [9] Hudson B., "Advanced Persistent Threats: Detection, Protection and Prevention", Sophos, 2013, p. 6. <https://www.lifeboatdistribution.com/content/vendor/sophos/whitepaper-sophos-advanced-persistent-threats-detection-protection-prevention.pdf>
- [10] *IBM Security Intelligence with Big Data*, <http://www-03.ibm.com/security/solution/intelligence-big-data/>
- [11] Jover R.P., Giura P., "How vulnerabilities in wireless networks can enable Advanced Persistent Threats", *International Journal on Information Technology (IREIT)*, No.1 (2) 2013, p. 145- 151, http://www.research.att.com/techdocs/TD_100739
- [12] Kim J., Lee T., Kim H., Park H., "Detection of Advanced Persistent Threat by Analyzing the Big Data Log", *Advanced Science and Technology Letters* 2013, vol. 29 (SecTech 2013), p. 32
- [13] *Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security Survey 2015*, PwC, 2014, http://www.pwccn.com/home/webmedia/635527689739110925/rcs_info_security2015.pdf
- [14] Muszynski J., Shipley G., "Narzedzia SIEM (Security Information and Event Management)", 2016, <http://www.computerworld.pl/news/325855/Narzedzia.SIEM.Security.Information.and.Event.Management.html>
- [15] Pietrzak P., „Jak skutecznie obslugiwac zaawansowane ataki APT (Advanced Persistent Threats)", <https://magazyn.mediarecovery.pl/jak-skutecznie-obslugiwac-zaawansowane-ataki-apt-tzw-advanced-persistent-threats>
- [16] Rot A., Sobinska M., "IT security threats in cloud computing sourcing model", M Ganzha, L Maciaszek, M Paprzycki (eds.) *Proceedings of the 2013 Federated Conference on Computer Science and Information*, PTI, Cracow 2013, fedcsis.org/proceedings/2013/pliks/fedcsis.pdf
- [17] Rot A., "Zarządzanie ryzykiem w cyberprzeżstrzeni – wybrane zagadnienia teorii i praktyki", *Projektowanie i realizacja systemow informatycznych zarzadzania. Wybrane aspekty*, Komorowski T.M., Swacha J. (eds.), Polish Information Processing Society PTI, Warsaw 2016
- [18] Rot A., "Enterprise Information Technology Security: Risk Management Perspective", *Proceedings of the World Congress on Engineering and Computer Science 2009*, Vol II, 2009, pp. 1171-1176
- [19] *Using Deep Learning To Detect Threat*, SignalSense, White Paper, p. 2. http://www.ten-inc.com/presentations/deep_learning.pdf
- [20] Virgillito D., "Cyber Crime Security Risks for Healthcare Companies", 2013, <http://massivealliance.com/2013/12/18/cyber-crime-security-risks-healthcare>
- [21] Why Should Enterprises Choose EventLog Analyzer as Their SIEM Solution? <https://www.manageengine.com/products/eventlog/manageengine-siem-whitepaper.html>
- [22] Zscaler Announces Comprehensive Cloud-based APT Solution, <https://www.zscaler.com/press/zscaler-announces-comprehensive-cloud-based-apt-solution>

A Modular Testbed for Intelligent Meters and their Ecosystem

Jan Wetzlich, Martin Nischwitz, Florian Thiel
 Physikalisch-Technische Bundesanstalt,
 Germany

Email: {jan.wetzlich, martin.nischwitz, florian.thiel}@ptb.de

Jean-Pierre Seifert
 Security in Telecommunications,
 Technische Universität Berlin,
 Germany

Email: jp.seifert@sec.t-labs.tu-berlin.de

Abstract—Modern, intelligent measuring systems are increasingly distributed and networked or even virtualized. In order to guarantee the security of the measurements, security gateways are an effective means of protecting the local sensors and displays from manipulations from public wide area networks. On the other hand this means a complex, tiered eco system, therefore we are setting up a testbed for conducting further research on this topic concerning new innovative security approaches beyond traditional public key infrastructure and their influence on system architectures, secure remote verification and legally conform update mechanisms.

I. INTRODUCTION

THE European Union is facing unprecedented challenges resulting from increased dependence on energy imports and scarce energy resources, and the need to limit climate change. Energy efficiency is a valuable means to address these challenges. It improves the Union’s security of supply by reducing primary energy consumption and decreasing energy imports. The conclusions of the European Council emphasised the need to increase energy efficiency in the Union to achieve the objective of saving 20 % of the Union’s primary energy consumption by 2020. To achieve this the European Commission has issued the directive 2012/27/EC [7] on energy efficiency which directly addresses energy end-use efficiency and energy services. A main statement is the introduction of intelligent energy meters to increase the awareness of the end-user about its consumption. Furthermore, the aim was formulated in the directive that at least 80 % of consumers should be equipped with intelligent metering systems by 2020. These energy meters are regulated within the framework of legal metrology.

Even only in Germany Legal Metrology covers around 160 million measuring instruments, which are used for business or administrative purposes or in the public interest. They are subdivided into 150 types of equipment, subassemblies and additional equipment. The largest share is attributable to the area of commodity meters, such as electricity, gas, water and heat meters. Other everyday points of contact with Legal Metrology include not only dispensing pumps at petrol stations and scales in the retail trade, but also speed and alcohol meters. The importance of adequate protection against tampering of the software in such measuring instruments can be seen in

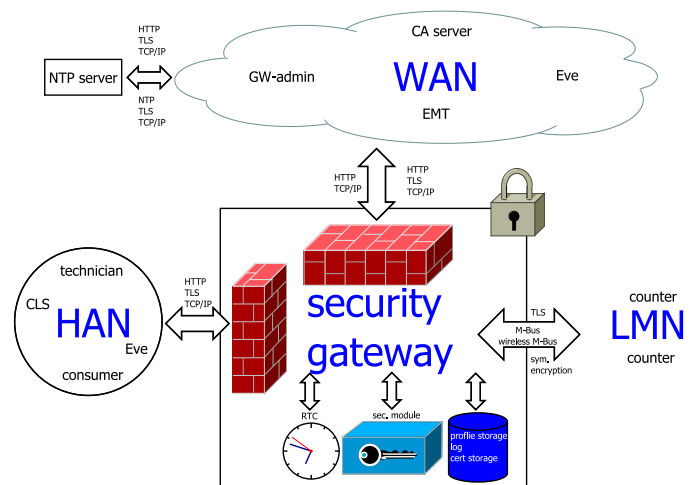


Fig. 1. Common entities in an ecosystem for intelligent meters covering an home area network (HAN) with some controllable local systems (CLS) connected to a wide area network (WAN) with external market participants (EMT) and a local metrological network (LMN) with different counters and meters

the proportion of the gross domestic product (GDP) generated by legal measurement: in most industrialized countries, legally relevant measurements are responsible for a share of 4% to 6% of GDP. This corresponds in Germany to an annual turnover of 104 to 157 billion Euros [1]. The consequences of successful manipulation can easily be estimated from these figures. At the same time, Legal Metrology is responsible for around 56% of the federal tax bill. In 2015, some 40 billion Euros was accounted for solely by revenue from the energy tax (electricity / gas / heat / mineral oil) [3].

Due to the strong trend towards digitalization, the share of software in measurement systems will grow steadily. At the same time, software already accounts for more than half of the development process in some measuring instruments. This evolution is accompanied by virtualization, networks and spacial distribution of sensors, data processing, data storage and monitoring. In Figure 1 a common example for such a system is shown. In order to guarantee the security of the measurements, security gateways are an effective means of protecting the local sensors and displays from manipulations from public broadband networks (WAN). In addition, there

are new technical possibilities for diagnostic tests as well as firmware updates from afar. Therefore a testbed for intelligent measuring systems is being developed at the PTB in cooperation with TU Berlin in order to investigate the associated processes and architectures scientifically.

In section II we discuss the legal framework for intelligent measuring instruments, section III presents the structure of the testbed ecosystem and the approach for the modeling testbed with its components and interfaces and finally section IV discusses targeted research in the field of intelligent measurement systems to be performed using the testbed.

II. LEGAL METROLOGY

The central concern of Legal Metrology is to protect and ensure trust in measurements. In this context, Legal Metrology does a lasting contribution to a functioning economic system by simultaneously protecting the consumers.

The International Organization of Legal Metrology (OIML) was set up to assist in harmonising such regulations across national boundaries to ensure that legal requirements do not lead to barriers in trade. Software requirements for this purpose are formulated in the OIML D 31 document [8]. WELMEC is the European committee to promote cooperation in the field of Legal Metrology, for example by establishing guides to help notified bodies (responsible for checking the measuring instruments) and manufacturers implement the Measuring Instruments Directive described below.

A. Legal European Framework

Directive 2014/32/EU of the European Parliament and of the Council [6], which is based on Directive 2004/22/EC [5], known as the Measuring Instruments Directive (MID), are directives by the European Union to establish a harmonized European market for measuring instruments, which are used in different member states. The aim of the MID is to protect the consumer and to create a basis for fair trade and trust in the public interest. The directive is limited to ten types of measuring instruments that have a special economic importance because of their number or their cross-border use. These are: water meters, gas meters and volume conversion devices, active electrical energy meters, heat meters, measuring systems for the continuous and dynamic measurement of quantities of liquids other than water, automatic weighing instruments, taximeters, material measures, dimensional measuring instruments, and exhaust gas analysers. The MID defines basic requirements for these measuring instruments, e.g. the protection against tampering and the display of billing-related readings. Each measuring instrument manufacturer themselves decide which technical solutions they want to apply. Nevertheless, they must prove to a notified body that their instrument complies to the MID requirements. The notified bodies that must be embraced by the manufacturers are denominated by the member states. In Germany, for example, the Physikalisch-Technische Bundesanstalt (PTB) is such a notified body. The PTB is furthermore the German national metrology institute providing additional scientific and technical services, which

is why it achieves the demanded technical expertise needed. In general, the combination of technical expertise related to the measuring instruments, competence for the assessment, monitoring of product related quality assurance systems, and experience with European regulations, are required. Additionally, it is of particular importance that the notified body is independent and impartial.

B. Critical Infrastructure

Commodity meters for gas, water and electrical energy are concerned to be parts of a critical infrastructure, which results in requirements of a high security level, but also the use of reliable, interoperable and trusted standards like [9].

III. APPROACH

The main idea is to highly use virtualization so that most parts of the testbed can be done in software. This provides higher flexibility for exchanging parts of the ecosystem and scaling to larger numbers of sensors etc. As a starting point we choose the eco system that is described by the technical directive TR-03109 from the German BSI [4]. In Figure 1 the composition of the ecosystem is shown. Only the gateway itself is implemented as a separate board. The main advantage of the chosen system is the opportunity to downscale this high level security system to use cases, where less security is mandatory or required. On the other side chosen system constitutes of traditional, state of the art concepts and technologies, including e.g. a public key infrastructure (PKI) and stateless webservices. Another side effect is the fact, that [4] will be mandatory for new electrical energy, water, gas and heat meters in Germany in the future, so there will be a huge dissemination of such systems. This means advancement, which can be easily integrated in the testbed or at least in a non disruptive manner, are more likely to be adopted.

A. Interfaces

In addition to the network interfaces, UART (TTL, RS232), RS485 / M-Bus, I2C and SPI as well as wireless M-Bus are available in the metrological network. The radio interface is implemented as a physical interface as well as via a channel simulation. With the help of the channel simulations, the system behavior can be investigated in the event of malfunctions and attacks on the wireless interfaces. The implemented simulated distortions include echoes, interference from other users of the ISM band, such as through home automation systems and forced collisions by simultaneous data transmission. For the manipulation of sensor signals and the interruption of physical interfaces, 4 digital to analog converters (DAC) and 16 DIO are available, which can switch further relays. By means of four analog-to-digital converters (ADC), any controllable devices can be tested for their reactions.

B. Sensors

The sensors of the measuring system are also simulated, which results in an independence from the measured physical variables. The virtualization approach allows the number of

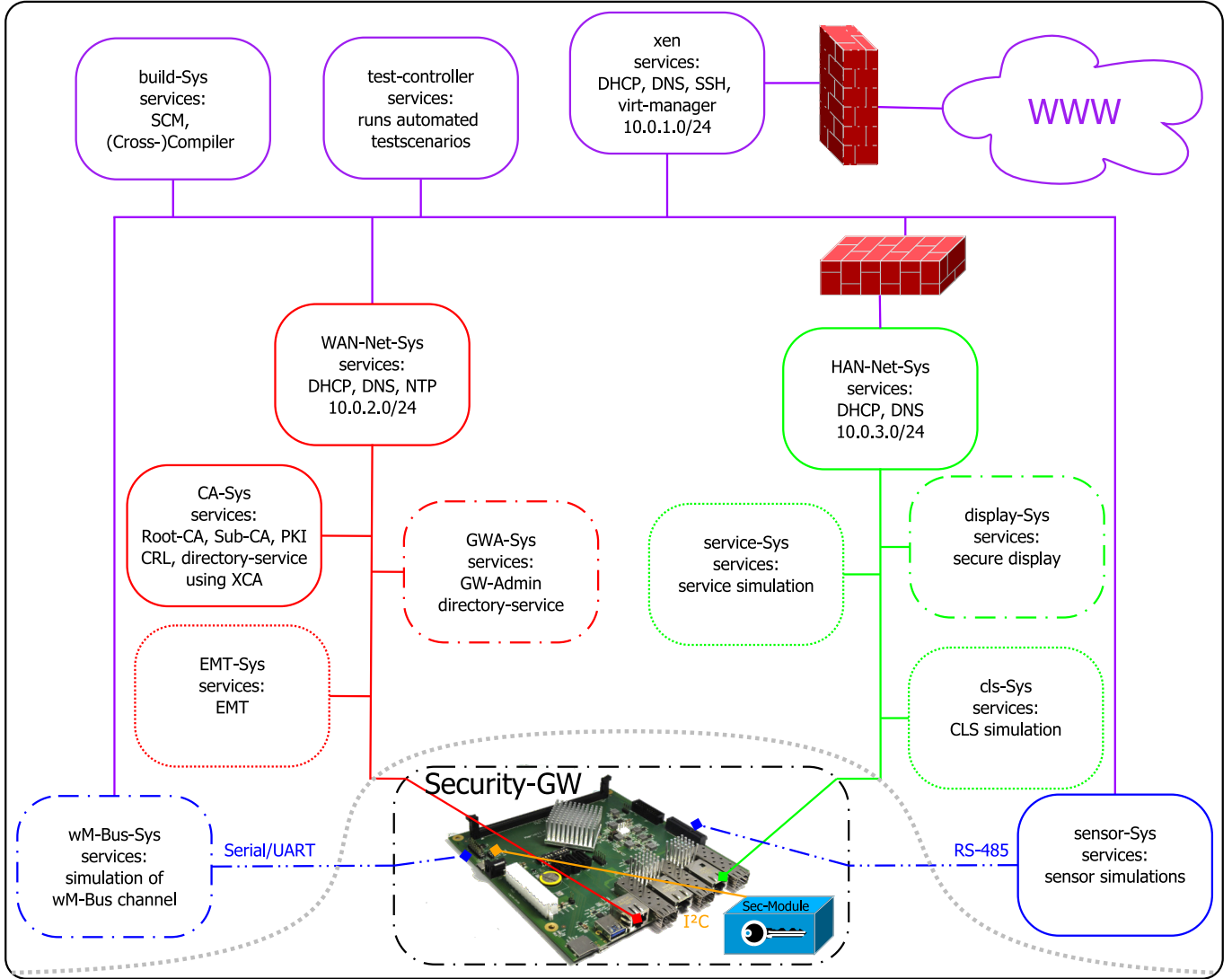


Fig. 2. Network layout of the ecosystem: HAN (green), WAN (red) and LMN (blue) are connected by the security gateway. For testing purposes there is an additional network around the eco system (purple).

sensors to be scaled and combined as desired. The configurable parameters of the basic behavior of the sensor simulation are:

- cyclic measurement data or incrementation rate for accumulative counters
- encryption type (plain/symmetrical AES/asymmetrical RSA or ECC)
- used credentials
- used interface (wireless M-Bus/M-Bus/RS232/I2C/SPI)
- parameters for the channel simulation(sending interval/obstacles)

The second possibility for controlling the sensor simulation is to dynamically manipulate the sensor during the execution of a test scenario. For example, it is possible to set counter readings, change keys, or interrupt the transmission or reception function at the interface to the gateway.

C. Network topology

The different networks of the ecosystem consist of wide area network (WAN) and a home area network. The WAN constitutes of a public key infrastructure, the gateway administrator, a system that provides general network services such as DNS, DHCP, NTP, as well as simulated external market participants. The local network also provides general network services with DNS and DHCP, in addition, a secure display, service technician and controllable systems are also connected here. In deviation from [4], there is also the possibility to connect sensors via network interfaces in the metrological network.

D. PKI

The initial version of the testbed constitutes of a traditional PKI with a single root certificate authority (root-CA) at the top, a tier with some subsequent CAs and at the bottom different

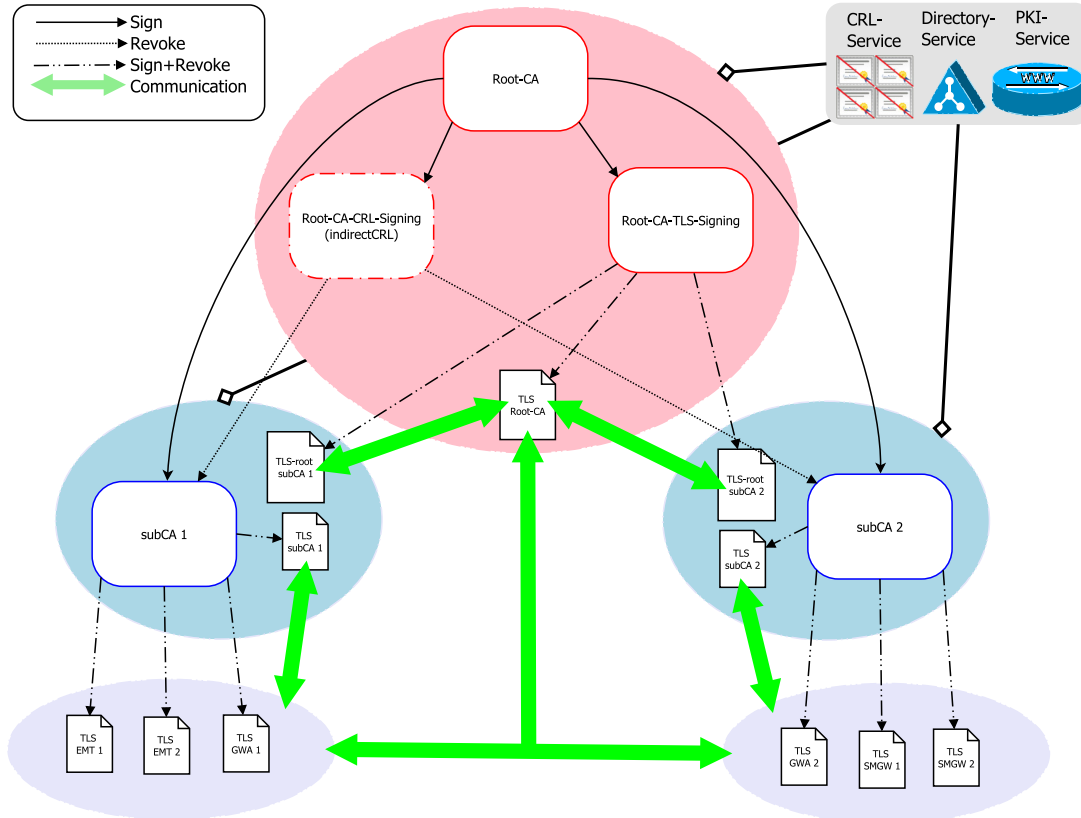


Fig. 3. The hierarchy of the implemented PKI.

certificate users e.g. GW admins, security gateways and TLS communication between CAs. The certificates are served via LDAP(s) and can be requested/issued via webservice. Signed certificate revocation list (CRL) are available via HTTP. The whole architecture is shown in Figure 3.

E. Test Automation

Running test scenarios is prepared by the test controller by establishing a defined output state and controlled by calling atomic methods of the test API during the course of the individual scenarios. The test scenarios are implemented for the greatest possible flexibility in Python. Figure 4 shows schematically the structure of the test API for a single component of the ecosystem. The test controller can access all components of the ecosystem, whereby the services and interfaces already provided by the component are addressed

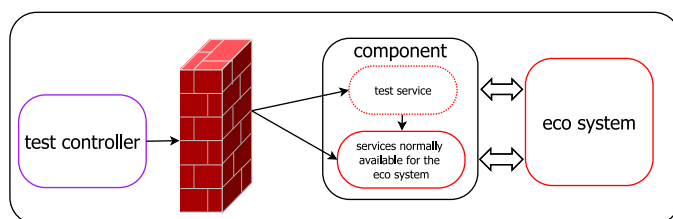


Fig. 4. Scheme of test API

preferably - for example, signing requests to the PKI. For more complex or non-existent methods, encapsulated extra test services are used on the component which, in turn, use existing services or interact directly with the ecosystem - for example, sending malicious data or requests or configuring new sensors in the gateway, this involves interactions with the gateway admin service, the gateway and possibly external market participants.

The test services are implemented on the side of the test controller as RESTful Webservices and are also written in Python. The third possible impact of the test controller on the ecosystem is manipulation using the analog and digital inputs and outputs, for example, to selectively switch off physically embedded components of the ecosystem, manipulate them or manipulate sensor inputs.

F. GW reference architecture

Based on [2] we chose a microkernel architecture for the security gateway on an ARMv8 board. A major goal of the reference architecture is the development and evaluation of safe methods for remote maintenance of intelligent measuring systems, as well as remote detection and verification.

Advantages: Due to the small-sized trusted computing base (TBC), the integrity of the entire gateway can reliably be ensured and verified by the targeted microkernel architecture with separated minimal systems. Possibly existing security gaps in parts of the software have significantly less impact

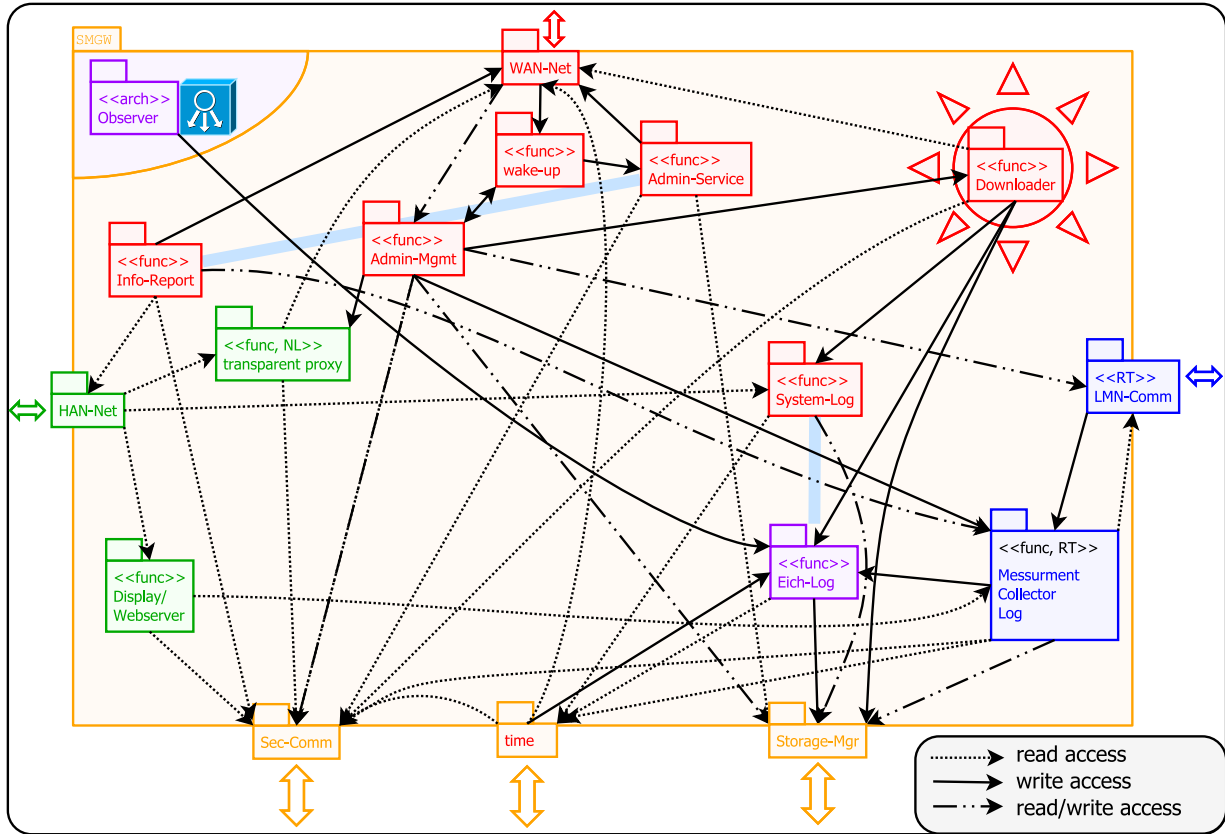


Fig. 5. Reference architecture for security gateway

on the overall system. A further advantage of the modular microkernel architecture is that the BSI TR-03109 (smart meter gateway with CC-certified security modules) can be used to scale the ecosystem as well as the gateway down to less sensitive measuring systems, in order to implement a protection level appropriate to the risk. The provided microkernel variants are, like all other components of the testbed opensource and thus particularly suitable as a reference architecture. In addition, virtualization enables existing applications to be run in a single virtual machine at a fast pace and then to be separated into individual virtual machines later.

Architecture design approach: In Figure 5 a possible partitioning for a security gateway is shown. In this case, conceivable functions, which have similar data streams, are combined into a virtual machine. Mainly these are the following functions:

- management service of the gateway itself
- informational services for the GW admin
- informational services for extern market participants
- informational services for local displays/devices in the HAN
- different system logs for users, admin and market authorities
- measurement data processing

In addition, an observer and a downloader are provided to monitor the integrity of the other virtual machines respectively

to update them remotely. It is common in such a microkernel architecture to outsource the operation of hardware interfaces such as persistent storage, network interfaces and other external interfaces into dedicated virtual machines. In Figure 5, this is represented for a gateway with a very high level of protection. With a lower protection requirement, individual virtual machines can be combined, which in turn reduces the hardware requirements for the measuring system.

As a first approach a microkernel of the L4 family was used here, however, due to the paravirtualization used, some adjustments of the drivers are necessary, so that in future work a microkernel will be used, which can use hardware virtualization functions of modern ARMv8 processors, so such modifications won't be needed.

IV. CONCLUSION AND OUTLOOK

The testbed is still work in progress, but main parts like the gateway, sensor simulation and PKI are already implemented. The completion of the testbed will be pursued for the end of the year.

A. Work still to do

The next steps include to develop and evaluate a suitable simulation for a set of controllable devices in the HAN as well as of service technicians in the local network and external market participants in the WAN. The test API can then be finalized and the test scenarios can be implemented.

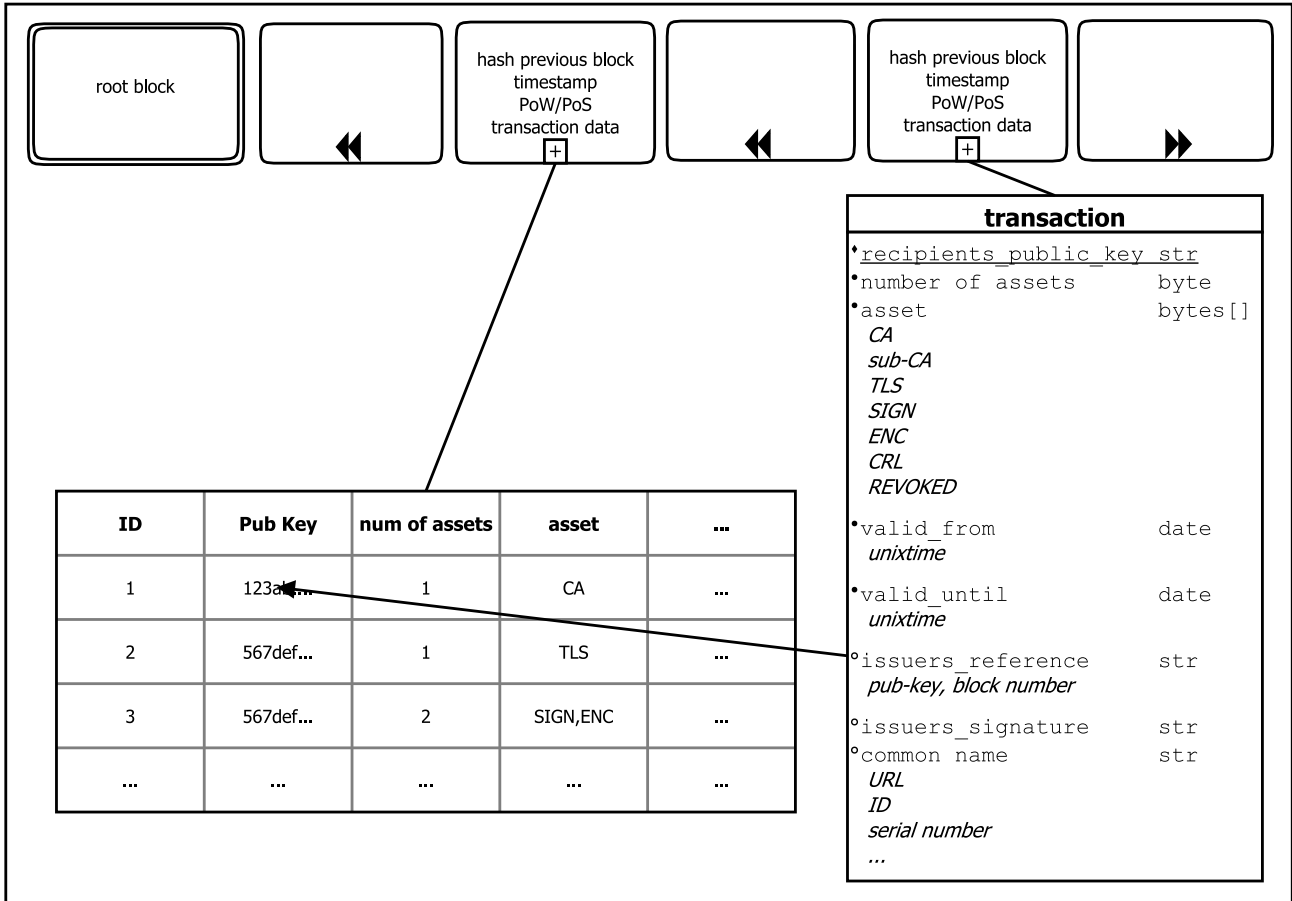


Fig. 6. Conceivable transaction scheme for asset granting and id verification using a blockchain.

B. Approaches beyond traditional PKI

The main research focus is to secure the data transfer using alternative approaches to a classical PKI with its limitations. such as Quantum Key Distribution [11] and post-quantum cryptography [12] for encryption, which is secure against quantum computer attacks, and blockchain for authentication without single point of failure.

Main advantages of replacing a traditional PKI by a blockchain are the greater reliability due to the distributed nature of a blockchain, as well as more transparent granting of assets/certificates. An other aspect might be the absence of a root-Key, so there will be no need for redistribution of a root-certificate. As a blockchain is subjected to computational and/or economical power of its node, a public blockchain might not be a suitable solution for a PKI in Legal Metrology, where only certain entities can be trusted to handle grant request with the required fidelity. A setup with a set of nodes limited to authorized participants like in Figure 7 appears to be a more preferable solution.

Common blockchains like Bitcoin [13] use a Proof-of-Work to overcome the consensus issue, but this implies huge computational effort and therefore huge energy consumption. Other approaches like Ethereum [16] use more energy-efficient proof of stake, which is usually defined by the possessed

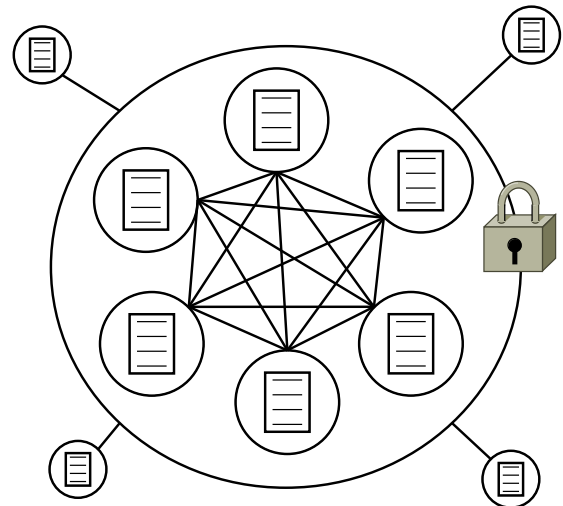


Fig. 7. Node topology for a private blockchain hosting a PKI. Inner nodes are granted to mine/mint transaction blocks outer nodes can only mirror the chain and may request assets to be confirmed by inner nodes

amount of an associated currency. This approach also seems to be less than ideal.

A proposed scheme for a blocklayout in a PKI chain is given

in Figure 6. We propose to include certificate revocations in the same chain as this will reduce complexity for clients and will give them a starting point for searching for revocations. Also a combination of a blockchain PKI with Physical Unclonable Function (PUF) [18] might be an interesting approach. Interesting and important questions might be:

- How can embedded devices handle the huge amount of data in such a blockchain for authentication?
- Proof-of-Work or an alternative?
- How to integrate PUFs into a blockchain?

C. Further Applications

Further research topics of interest beside approaches beyond traditional PKI focus on new opportunities due to the permanent or at least regular network connection of intelligent measuring systems, such as:

remote verification, remote update: Subsequent investigations will deal in particular with the trustworthy remote partial examination as well as with safe remote software upgrades of intelligent measuring systems. It's expected to develop a legal conform reference method or solution therefore.

smart services: The third object of investigation is research on novel services, which are based on the accumulated data of intelligent measuring systems. For example, methods for predictive maintenance or for identifying attacks on networked measuring systems are conceivable. Here again blockchain approaches for smart contracts might be a suitable solution especially if blockchain technology is already used for PKI.

REFERENCES

- [1] D. Peters, M. Peter, J.-P. Seifert und F. Thiel: A Secure System Architecture for Measuring Instruments in Legal Metrology, published in Computers, Open Access Journal (ISSN 2073-431X), 2015
- [2] D. Peters, F. Thiel, M. Peter, J.-P. Seifert, "A Secure Software Framework for Measuring Instruments in Legal Metrology", accepted for IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Pisa, Italy, May 11-14, 2015
- [3] N. Leffler and F. Thiel. Im Geschäftsverkehr das richtige Maß. In Schlaglichter der Wirtschaftspolitik, Monatsbericht November, 2013.
- [4] BSI TR-03109 Technische Vorgaben für intelligente Messsysteme und deren sicherer Betrieb, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR03109.pdf?__blob=publicationFile&v=3
- [5] Directive 2004/22/EC of the European Parliament and of the Council, March 2004. Official Journal of the European Union.
- [6] Directive 2014/32/EU of the European Parliament and of the Council, October 2013. Official Journal of the European Union. doi: 10.3000/19770677.L_2014.096.eng.
- [7] Directive 2012/27/EU of the European Parliament and of the Council, February 2014. Official Journal of the European Union. doi: 10.3000/19770677.L_2012.315.eng
- [8] General requirements for software controlled measuring instruments, 2008. OIML D 31.
- [9] CEN-CENELEC-ETSI Technical Report TR 50572:2011, ICS 33.200; 91.140.01
- [10] Oppermann, Alexander and Seifert, Jean-Pierre and Thiel, Florian. 2016. Distributed Metrological Sensors managed by a secure Cloud-Infrastructure, accepted for 18. GMA/ITG Fachtagung, Sensoren und Messsysteme 2016, Nürnberg, 10.-11. Mai, (2016)
- [11] P Eraerds, N Walenta, M Legré, N Gisin, and H Zbinden. Quantum key distribution and 1 gbps data encryption over a single fibre. *New Journal of Physics*, 12(6):063027, 2010.
- [12] Daniel J. Bernstein. *Introduction to post-quantum cryptography*, pages 1–14. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.
- [13] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. <http://bitcoin.org/bitcoin.pdf>.
- [14] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, and Luca Spalazzi. Certificate validation through public ledgers and blockchains. pages 156–165.
- [15] Edoardo Gaetani, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. Blockchain-based database to ensure data integrity in cloud computing environments. pages 146–155.
- [16] Elfriede Sixt. *Ethereum*, pages 189–194. Springer Fachmedien Wiesbaden, Wiesbaden, 2017.
- [17] Alexander Chepurmoy. Interactive proof-of-stake. *CoRR*, abs/1601.00275, 2016.
- [18] W. Che, F. Saqib, and J. Plusquellic. Puf-based authentication. In *2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pages 337–344, Nov 2015.

1st Workshop on Internet of Things—Enablers, Challenges and Applications

THE Internet of Things is a technology which is rapidly emerging the world. IoT applications include: smart city initiatives, wearable devices aimed to real-time health monitoring, smart homes and buildings, smart vehicles, environment monitoring, intelligent border protection, logistics support. The Internet of Things is a paradigm that assumes a pervasive presence in the environment of many smart things, including sensors, actuators, embedded systems and other similar devices. Widespread connectivity, getting cheaper smart devices and a great demand for data, testify to that the IoT will continue to grow by leaps and bounds. The business models of various industries are being redesigned on basis of the IoT paradigm. But the successful deployment of the IoT is conditioned by the progress in solving many problems. These issues are as the following:

- The integration of heterogeneous sensors and systems with different technologies taking account environmental constraints, and data confidentiality levels;
- Big challenges on information management for the applications of IoT in different fields (trustworthiness, provenance, privacy);
- Security challenges related to co-existence and interconnection of many IoT networks;
- Challenges related to reliability and dependability, especially when the IoT becomes the mission critical component;
- Zero-configuration or other convenient approaches to simplify the deployment and configuration of IoT and self-healing of IoT networks;
- Knowledge discovery, especially semantic and syntactical discovering of the information from data provided by IoT;

The IoT conference is seeking original, high quality research papers related to such topics. The conference will also solicit papers about current implementation efforts, research results, as well as position statements from industry and academia regarding applications of IoT. The focus areas will be, but not limited to, the challenges on networking and information management, security and ensuring privacy, logistics, situation awareness, and medical care.

TOPICS

The IoT conference is seeking original, high quality research papers related to following topics:

- Future communication technologies (Future Internet; Wireless Sensor Networks; Web-services, 5G, 4G, LTE, LTE-Advanced; WLAN, WPAN; Small cell Networks...) for IoT,

- Intelligent Internet Communication,
- IoT Standards,
- Networking Technologies for IoT,
- Protocols and Algorithms for IoT,
- Self-Organization and Self-Healing of IoT Networks,
- Trust, Identity Management and Object Recognition,
- Object Naming, Security and Privacy in the IoT Environment,
- Security Issues of IoT,
- Integration of Heterogeneous Networks, Sensors and Systems,
- Context Modeling, Reasoning and Context-aware Computing,
- Fault-Tolerant Networking for Content Dissemination,
- Architecture Design, Interoperability and Technologies,
- Data or Power Management for IoT,
- Fog—Cloud Interactions and Enabling Protocols,
- Reliability and Dependability of mission critical IoT,
- Unmanned-Aerial-Vehicles (UAV) Platforms, Swarms and Networking,
- Data Analytics for IoT,
- Artificial Intelligence and IoT,
- Applications of IoT (Healthcare, Military, Logistics, Supply Chains, Agriculture, ...),
- E-commerce and IoT.

The conference will also solicit papers about current implementation efforts, research results, as well as position statements from industry and academia regarding applications of IoT. Focus areas will be, but not limited to above mentioned topics.

SECTION EDITORS

- **Cao, Ning**, College of Information Engineering, Qingdao Binhai University
- **Furtak, Janusz**, Military University of Technology, Poland
- **Zieliński, Zbigniew**, Military University of Technology, Poland

REVIEWERS

- **Amanowicz, Marek**, Military University of Technology
- **Antkiewicz, Ryszard**, Military University of Technology, Poland
- **Chudzikiewicz, Jan**, Military University of Technology in Warsaw, Poland
- **Cui, Huanqing**, Shandong University of Science and Technology, China

- **Ding, Jianrui**, Harbin Institute of Technology, China
- **Fouchal, Hacene**, University of Reims Champagne-Ardenne, France
- **Fuchs, Christoph**, Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE, Germany
- **Ghamri-Doudane, Yacine**, Université La Rochelle
- **Gluhak, Alexander**, Intel Labs Europe
- **Higgs, Russell**, University College Dublin, Ireland
- **Hodoň, Michal**, University of Žilina, Slovakia
- **Johnsen, Frank Trethan**, Norwegian Defence Research Establishment (FFI), Norway
- **Krco, Srdjan**, DunavNET
- **Lenk, Peter**, NATO Communications and Information Agency, Other
- **Li, Guofu**, University of Shanghai for Science and Technology, China
- **Ma, Fumin**, Nanjing University of Finance and Economics, China
- **Marks, Michał**, NASK - Research and Academic Computer Network, Poland
- **Murawski, Krzysztof**, Military University of Technology, Poland
- **Niewiadomska-Szynkiewicz, Ewa**, Research and Academic Computer Network (NASK), Institute of Control and Computation Engineering, Warsaw University of Technology
- **Paprzycki, Marcin**, Systems Research Institute Polish Academy of Sciences, Poland
- **Sabir, Essaid**, Hassan II University of Casablanca
- **Sikora, Andrzej**, Research and Academic Computer Network (NASK)
- **Skarmeta, Antonio**, University of Murcia
- **Suri, Niranjana**, Institute of Human and Machine Cognition
- **Wrona, Konrad**, NATO Communications and Information Agency
- **Xu, Jian**, Northeastern University, China
- **Xu, Lina**, University College Dublin, Ireland
- **Zhang, Tengfei**, Nanjing University of Post and Telecommunication, China
- **Zhao, Yongbin**, Shijiazhuang Tiedao University, China
- **Zheng, Lijuan**, Shijiazhuang Tiedao University, China
- **Zhou, Wei**, Qingdao Technological University, China

Assessment of Feasible Methods Used by the Health Care Industry for Real Time Location

J Pancham
Department of IT, Durban
University of Technology
Durban, South Africa
Email: panchamj@dut.ac.za

Richard Millham
Department of IT, Durban
University of Technology
Durban, South Africa
Email: richardm1@dut.ac.za

Simon James Fong
Department of Computer and
Information Science University of
Macau, Macau SAR
ccfong@umac.mo

Abstract—This position paper surveys relevant literature in order to evaluate Real Time Location System (RTLS) for the health care sector. The first step is to identify the most common aspects required for a feasible health care implementation. The second step is to utilise these identified criteria to evaluate common RTLS technologies. The most feasible technology matching these criteria will be selected. Because the most feasible technology selected from the evaluation may lack one or more of the most common identified aspects for a healthcare RTLS, enhancements of this technology will be proposed to overcome these limitations.

Index Terms—Real time location system, RTLS, RFID, Health Care, Bluetooth low energy networks

I. INTRODUCTION

ALTHOUGH the capability to track both people and objects outdoors is achievable without difficulty by the use of Global Positioning (GPS) technology, there is also a need to determine the location of people and objects indoors at real time with a high degree of accuracy. Indoor tracking is not feasible through GPS technology [1], due to the dependence on a link between the GPS device and the positional satellites. Consequently, new methods need to be evaluated for indoor tracking. A number of researchers and practitioners have used RTLS for a number of years to address indoor localization in various sectors. According to the definition by [2], an RTLS is a “combination of hardware and software that is used to continuously determine and provide the real time position of assets and resources equipped with devices designed to operate with the system”.

The main focus of this research is on the application of RTLS in health care. Within the health care environment researchers are investigating feasible technologies for patient and asset location. These two applications are similar in all respects except for the method of attachment of the device to the asset or patient. Well-managed implementations of RTLS solutions within the health care sector can deliver tremendous value for patient management [3] and [4]; and improved general health care [5]. In addition other important benefits in using RTLS are asset management for easy location of equipment [4] within a health care environment. The results of a survey of the largest public health facility in state of Florida conducted by [6] showed that real time patient monitoring was one of two priorities followed by loca-

tion and tracking of medical equipment. In health care there are various constraints, important ones include prevention of interference with the functioning of any medical equipment [7], low cost in terms of price and low transmission power [8]. Furthermore, the selected hospital which forms the exemplar of the RTLS requirements has additional constraints of maximizing battery life, utilizing small form factor devices that can be worn by patients and be able to be used in a scalable variable patient and space environment. The remainder of the concept paper is organized as follows: methodology, results, discussion and conclusion.

II. METHOD

The methodology employed utilized a literature exploration to ascertain the methods currently used in the health care sector for indoor RTLS. The literature resulting from this exploration was examined to assess these methods and / or technologies in terms the limitations posed by both the health care field and the hospital exemplar.

A. Research Questions

- The research questions (RQ) addressed by this study are:
- RQ1. Based on the literature review and hospital exemplar which set of attributes can be identified for an RTLS in health care?
 - RQ2. Given these identified attributes what common technologies are most feasible in health care with respect to these attributes?

B. Search Process

The relevant literature was selected using combinations of several expressions on prominent databases containing scholarly publications such as Google Scholar, Elsevier (SCOPUS) and IEEE [9]. The reason for the choice of these databases is that they were readily accessible to the researchers. Key phrases such as “RTLS in healthcare”, “low energy localization in healthcare”, “patient real time location systems” were used on these search engines and databases.

C. Delimitation: Inclusion and exclusion criteria

Due to the rapid advances in of technology, and also to ensure that the latest technologies were assessed, the authors limited the time span of papers in chapters of periodicals,

journals, and congress proceedings published predominantly between 2012 and 2017. Possible other constraints include backdated articles within this time span, articles not being available due to indexing issues, and only English language articles being chosen. Despite these constraints, it is understood that this study has attained an acceptable appraisal of the chief RTLS systems. This review is not a comprehensive publication appraisal nor a systematic literature review of all scientific literature of the RTLS field, only the most popular RTLS research technologies are presented. These most popular technologies were selected to give some noteworthy descriptive instances of RTLS published in recent peer reviewed works.

From the literature survey the most appropriate attributes in terms of RTLS and exemplar constraints were identified. The health care sector has other constraints such as electromagnetic interference [8], [7] and scalability [10], but space constraints limited our selection to the most appropriate and the most common attributes. In addition to the exemplar of a hospital survey data of 23 US hospitals [11] was used in the evaluation process.

D. Analysis

The chosen technologies were assessed against these identified characteristics. Several technologies such as Ultra wide Band [12], infrared, ultrasonic, standard TV signals, computer vision physical contact [13] for health care RTLS were not considered as these do not closely meet the minimum criteria of the essential characteristics such as reasonable cost.

III. RESULTS

A. Identified attributes

We identified five main attributes viz. cost [14], energy consumption [15], detection range [14], size and accuracy [12]. Another attribute scalability is an important factor for consideration as determined by the exemplar. Due to space constraints other attributes such as security were not included in the study. The main criteria identified were used to compare the different principle technologies, these being RFID, Bluetooth and BLE and Wi-Fi. These are discussed together with their advantages and shortcomings. A number of other technologies such as Ultra wide Band [12], which can be used for localization, they were not considered due to the nature of the environment and its constraints.

B. Technologies

1) RFID

Despite the extensive research by academics to assist in designing and improving RFID systems over the number of years of the existence of RFID, there are still remains issues that need to be resolved. An RFID tag consists of two components: an antennae that is used to send and receive data and a chip that stores information about the item being tracked [16]. The RFID tag can be classified into three categories viz. passive, semi-passive and active. Active and

semi-passive RFID tags have batteries to power their circuits. These active tag uses its battery power source to broadcast radio waves to a reader, whereas a semi-passive tag relies on an external power source i.e. the reader to supply power for its broadcasting. A passive tag on the other hand is composed of an antenna coil and a silicon chip that includes basic modulation circuitry and non-volatile memory. These passive tags rely entirely on the reader to power the tag which then send its unique identifier [17].

RFID tags are used in numerous applications such as health care and retail. [16] identified two technical issues with RFID viz. tag collision where readers read multiple tags at the same time and are unable to determine the individual identities involved and reader collision where multiple readers read a tag. These technical issues impact negatively on the accuracy of detection. Other issues identified were privacy and signal interference [7]. However, although privacy is an important aspect to be considered in the health care environment, in this case we do not consider any personal or health related information. Signal interference is considered whilst the main attributes identified at being evaluated.

[4] conducted an extensive review of 215 research articles dealing with RFID applications and issues in healthcare. Their findings revealed that the full benefit of using RFID technology will depend on different factors including cost.

An additional problem identified by [16] is that many models based on academic research are not implementable and therefore do not help the practitioner. Even when implemented a number of challenges plague the industry preventing wide scale rollout. The main limitations in the implementation of RFID identified by [6] include technical problems such as distractions by metallic objects and electromagnetic interference in reading tags affecting detection range and accuracy as well as the high cost of infrastructure and tags. Solutions to resolve these challenges come at a high cost limiting their feasibility of wide scale implementation.

[6] analysis reveals that cost is an important barrier in RTLS for locating and monitoring of both patients and assets. This conclusion is in agreement with previous research by [18] who found that cost was also an important barrier for both non-implementers and future implementers of RTLS in particular with RFID.

Although the cost of passive tags is low [13] they require more readers as they need to be detected at a very close range, hence increasing total cost. In comparison to passive RFID tags, active RFID tags are more expensive but the accuracy increases to between 1 and 2 meters [12]. Consequently the accuracy of the detection as well as detection range will be dependent on the type of tag being used. Energy consumption is medium as some batteries can have lifespan ranging from months up to a year. However, the size of the device becomes bulky once the battery and holder is fastened.

2) Bluetooth

A popular wireless technology used for exchanging data over short distances is Bluetooth. A number of different techniques such as Received Signal Strength Indication (RSSI), trilateration [19] or finger printing are used to increase accuracy for determining location. Accuracy for location differs at a cost in term of power consumption, size of device, and other factors. A number of different methodologies exist to increase the accuracy, the most popular being the RSSI technique which increases accuracy to 1-2 (meters) [20]. An available improvement of RSSI involves a Kamlan filter which increases Bluetooth accuracy to 0.47m but at a cost of increased size (due to larger storage requirements) and increased power consumption [14]. As can be seen these RSSI and Kamlan filter techniques adds to the size form factor for Bluetooth and energy consumption. An example of Bluetooth system is Bluetooth Local Infotainment Point (BLIP) which is a managed network offering access to LAN / WAN via Bluetooth [13].

Bluetooth also has drawbacks in crowded areas due to signal attenuation and interference. Bluetooth can transfer large quantities of data, but consumes battery life quickly and costs a lot more [21]. This gave birth to Bluetooth Low Energy (BLE) suitable to exchange little amounts of data consuming using lower energy at a cheaper cost.

3) BLE

BLE is the power-version of Bluetooth that was built for the Internet of Things (IoT) making it perfect for devices that run for long periods on power sources, such as coin cell batteries or energy-harvesting devices [22]. One of the two systems of this version is Bluetooth low energy which transmits small packets of data whilst consuming significantly less power than the previous version of Bluetooth [15]. A BLE system typically consists of a stationary anchor that detect the tags; a tag; and a location engine to calculate the location of the tag [23]. BLE is an improvement and a later version of Bluetooth (BT) offering several advantages such as smaller form factor, lower cost and extended coverage. [24] in their research recognized that the point-to-point communication of the current BLE nodes has only limited coverage over a short range. They propose using a wireless mesh multi-hop network that has multiple nodes that are capable of communicating with each other to enable routing of packets to extend this limited coverage as a possible solution. This distance can be extended further with the combination of current technologies that are more efficient.

Bluetooth® 5 released on 6 December 2016 is a transformative update on previous versions that significantly increases the range, speed and broadcast messaging capacity of Bluetooth applications. This version quadruples range and doubles speed of low energy connections while increasing the capacity of connectionless data broadcasts by eight times [25].

4) Wi-Fi

The concept behind Wi-Fi RTLS is that this technology can utilize the existing Wi-Fi infrastructure to communicate with Wi-Fi tags [17]. In order to use Wi-Fi for RTLS

additional Wi-Fi access points will need to be installed for a reasonable detection to achieve real time object or people tracking. Wi-Fi is used widely indoors and provides connectivity for a large number of devices. The basic architecture consists of a Wireless Access Point (WAP) and a Wi-Fi device which contains a Wi-Fi module for connectivity. The cost of devices that connect with the WAP will depend on the functionality provided. However the length of battery life will be very low. RTLS uses a single WAP to detect Wi-Fi tags and users Time Difference of Arrival (TDoA) and RSSI to calculate location [17]. The detection accuracy is approximately 3M [26], [12]. Examples of Wi-Fi solutions using Wi-Fi are Ekahau, Microsoft research radar, AeroScout, Intel Place Lab and Pinpoint 3D [13].

The location accuracy for Wi-Fi can be defined as zone, room or subroom level. Even in some cases Wi-Fi tags will be incorrectly detected in a room and to compound this signals cannot be detected by moving assets because of obstructions between the tag and access points [17].

C. Evaluation of Technologies

The work by [23], which investigated the reliable tracking of people acknowledged the problems of multipath fading and shadowing often leading to companies using multiple technologies to eliminate the respective disadvantages. Their results showed that detection was unreliable for boundary conditions especially in penetrable walls whilst results were more reliable when tags were closer to the anchors. Hence they concluded that more work was required to improve accuracy.

[27] in their research recommended that further work is needed to investigate alternative systems with lower power consumption and improved accuracy of localization tracking for the health care sector. They also identified optimizing the size and battery life as challenges facing an optimal RTLS.

Due to the complexity for rating total cost, size of devices and energy consumption a total relative rating was used. The measurements for detection range and accuracy are dependent on the type of tag and hardware used. Therefore measurements will have a wide range and will vary depending on the infrastructure used. The technologies selected are the most appropriate for RTLS within a health care environment. The following are key considerations for the different technologies: cost due to the tight budgets of health care institutions, size because the tag will be worn by patients, energy consumption to ensure long battery life as well as enabling the battery to be as small as possible, accuracy to correctly locate a patient or asset and detection range to minimize infrastructure.

The results of the evaluation of 23 hospitals by [11] are indicated in Table 1. Furthermore, it was noted that at the time of the survey only eleven hospitals had systems that were fully operational. Although this can be attributed to various reasons, one of the claims by the vendors is that the systems failed to deliver the precision of systems promised. Future research is required to ensure that detection accuracy

claims are consistent. The author further claimed that research projects to improve RTLS are not proven beyond the pilot phases or lab experiments in holistic hospital environments [26].

TABLE 1 RESULTS OF US HOSPITAL SURVEY

Technology used	No of hospitals	No of hospitals / Degree of accuracy
RFID	17	Low = 7, Medium = 8
Ultrasound	3	Medium = 3
Zigbee	2	Medium = 1, High = 1
IR	1	High = 1
UWB	1	Low = 1

The attributes for RFID depend on the tag type (active or passive) and their related equipment [13], [14]. The cost of Bluetooth and BLE modules are both low whilst the cost of Wi-Fi is medium to high [13]. The cost of Bluetooth and BLE is lower compared to Wi-Fi [13]. The detection range is between 50 and 100 meters for Bluetooth. The accuracy for Wi-Fi is 10 to 20 meters [12] compared to 10cm to 10

meters for Bluetooth [13], [14]. BLE on the other hand has an accuracy of 3cm to 5 meters [28]. Scalability is generally good for all technologies as noted by [13].

The following legend is used for Table 2 due to space constraints:

EC: Energy Consumption;

DR: Detection Range;

Cost and Energy Consumption constraints: L-Low, M-Medium, H-High;

Size: S-Small, M-Medium, L-Large

IV. DISCUSSION

RTLS in health care will enable efficient location of patients, employees and equipment. Although RTLS have realized benefits in some cases further research is required to reduce the serious technical impediments to its implementation with regards to asset management [11]. After an evaluation of the technologies as per the identified attributes listed in Table 2 together with more recent update to and promises by Bluetooth 5 technology [25], BLE was determined as the most appropriate and feasible technology for the purposes of

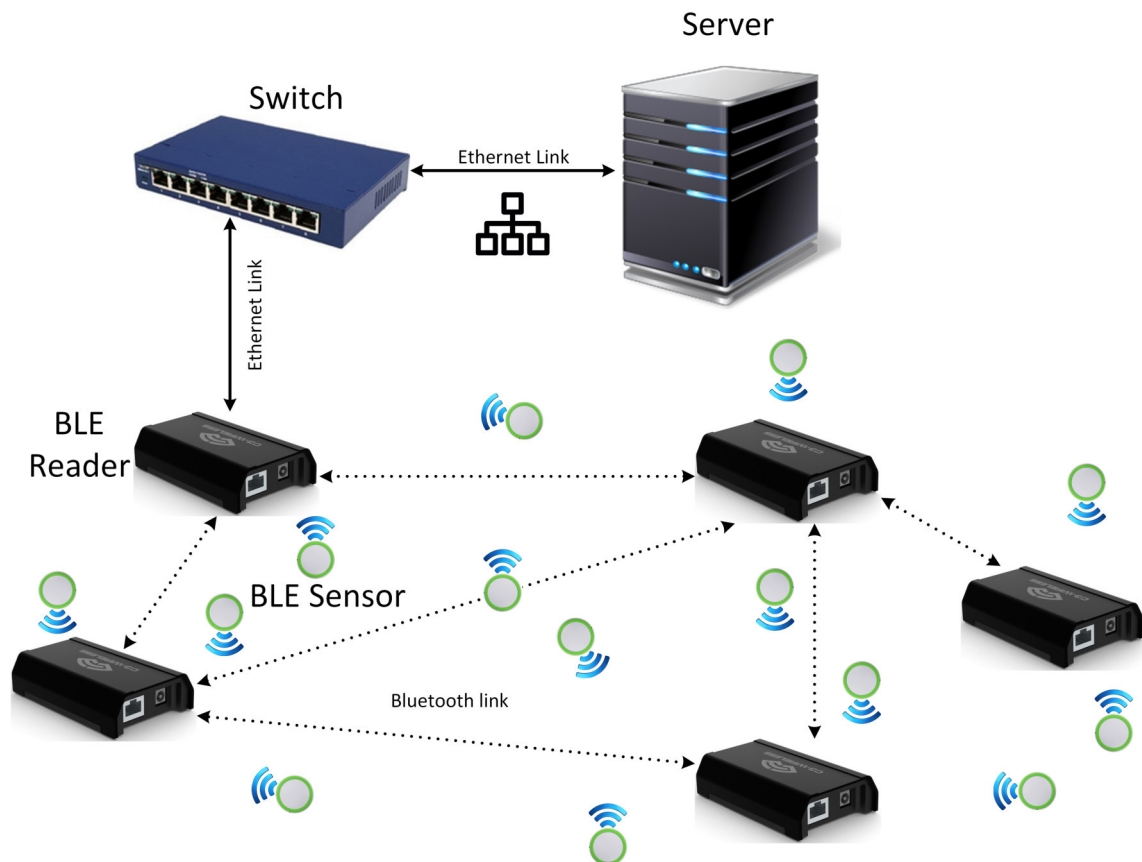


Fig. 1. BLE Network Architecture

TABLE 2 TECHNOLOGY ATTRIBUTES

Tech	Cost	EC	DR	Size	Accuracy	Scalability
RFID	H	M	Depends on Tag type	L	Depends on Tag type	Good with minimum of 2 tags
BT	M	M	100M for class 1	S	10cm to 10M	Good
BLE	L	L	High (50M)	S	3cm to 5M	Good
Wi-Fi	M	H	up to 200M	L	10 to 20M	Good

patient and asset tracking for a health care environment. An example of this is that BLE can be configured into a low cost low energy network architecture enabling lower energy consumption [29] and extending the range. The use of BLE devices, with low power consumption will extend battery life thereby reducing maintenance. [30] due to the high volume of patients as well as the size of hospitals especially those in the public sector cost is an important constraint. Therefore these factors were some of the main factors in selecting the most appropriate technology. However BLE suffers from the issues of small detection range and varying degrees of accuracy. Although security is often considered as an important aspect in healthcare, this will need to follow guidelines e.g. (hl7) as set by the health care industry. This will be taken into account during further research.

A combination of BLE tags and BLE readers is required to comply with the requirements for the health care environment.

The BLE reader could be powered by a battery to allow for flexibility and mobility as well as installation of power infrastructure. BLE tags will communicate to BLE readers via blue tooth. The BLE reader will have capability to link to a network switch via an Ethernet cable or a Wi-Fi link. Wi-Fi should prove to be a less disruptive option to be used in the architecture for connectivity back to a server. BLE readers will communicate with each other via Bluetooth and will eventually link back to the switch. A BLE reader can communicate to multiple readers via multiple paths to form a mesh network to cater for redundancy in case of failure of a BLE reader. This high level architecture is depicted in Figure 1. Using this high level architecture, the BLE tags will be connected to a server via the network.

The complexity of the communication and redundancy is housed in the BLE reader so that the BLE tag is less complex reducing its power consumption and cost. BLE readers will be mounted at fixed locations and can therefore have much larger batteries and / or be connected to a power source. The BLE tag will link to the closest BLE readers from which their location can be calculated using a combination of methods. The accuracy of the location required will depend on the usage. Therefore the above configuration

allows for a flexible implementation depending on the accuracy required.

After the selection of these technologies which are seen as the most suitable, enhancements involving identifying and implementing appropriate methods to function better in the selected hospital in order to study a live implementation in the practical setting were proposed.

V. CONCLUSION

An accurate and reliable RTLS system within the constraints of the health care environment requires a well-designed architecture. In order to address the challenges identified our approach is to use a combination of BLE tags (sensor) and readers with suitable algorithms to demonstrate the feasibility of an RTLS that mitigates these challenges. A network algorithm will be designed to find the best possible paths in terms of through put, load balancing, and power consumption for communication between BLE tags and BLE readers as well as between the readers. The communication between the different BLE readers in a mesh network will enable coverage of the blind spots not covered by the other readers and will extend the network coverage to increase detection range and improve accuracy as shown in Figure 1. A combination of multiple methods such as triangulation, fingerprinting [31], block chain architecture and repeater tags (tags configured to forward messages) will be used to increase the location accuracy whilst minimizing energy consumption. The availability of multiple communication paths will ensure scalability. By adopting a combination of techniques to improve accuracy and detection range, this might be at the cost of increased complexity, size, and power consumption. This will result in the increase of the cost of the device. Therefore future work will attempt to establish a balance between the primary identified factors

The primary focus of this evaluation was to analyze the relevant literature in the field and to evaluate the technologies for their advantages and disadvantages based on a set of attribute criteria as determined by the literature. Based on this evaluation, the authors selected the most appropriate technology and proposed solutions that addressed their identified shortcomings. Once the pilot sites have been tested the final results will be published in subsequent research articles.

REFERENCES

[1] S. Kim, S. Ha, A. Saad, and J. Kim, "Indoor positioning system techniques and security," in *e-Technologies and Networks for Development (ICeND), 2015 Forth International Conference on*, 2015, pp. 1-4.

[2] International Standards Organization (ISO), "Information technology - Automatic identification and data capture (AIDC) techniques - Harmonized vocabulary - Part 5: Locating systems," vol. ISO/IEC 19762-5, ed. Geneva: ISO, 2007.

[3] N. M. Potisek, R. M. Malone, B. B. Shilliday, T. J. Ives, P. R. Chelminski, D. A. DeWalt, *et al.*, "Use of patient flow analysis to improve patient visit efficiency by decreasing wait time in a primary care-based disease management programs for anticoagulation and chronic pain: a quality improvement study," *BMC health services research*, vol. 7, p. 8, 2007.

- [4] S. F. Wamba, A. Anand, and L. Carter, "A literature review of RFID-enabled healthcare applications and issues," *International Journal of Information Management*, vol. 33, pp. 875-891, 2013.
- [5] M. Attarha and N. Modiri, "Focusing on the importance and the role of requirement engineering," in *the 4th International Conference on Interaction Sciences (ICIS)*, Busan, Korea, 2011, pp. 181-184.
- [6] H. J. Yazici, "An exploratory analysis of hospital perspectives on real time information requirements and perceived benefits of RFID technology for future adoption," *International Journal of Information Management*, vol. 34, pp. 603-621, 2014.
- [7] W. Yao, C.-H. Chu, and Z. Li, "The adoption and implementation of RFID technologies in healthcare: a literature review," *Journal of medical systems*, vol. 36, pp. 3507-3525, 2012.
- [8] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," *Computer Networks*, vol. 54, pp. 2688-2710, 2010.
- [9] S. Keele, "Guidelines for performing systematic literature reviews in software engineering," in *Technical report, Ver. 2.3 EBSE Technical Report. EBSE*, ed: sn, 2007.
- [10] M. N. K. Boulos and G. Berry, "Real-time locating systems (RTLS) in healthcare: a condensed primer," *International journal of health geographics*, vol. 11, p. 25, 2012.
- [11] J. A. Fisher and T. Monahan, "Evaluation of real-time location systems in their hospital contexts," *International journal of medical informatics*, vol. 81, pp. 705-712, 2012.
- [12] Z. Deng, Y. Yu, X. Yuan, N. Wan, and L. Yang, "Situation and development tendency of indoor positioning," *China Communications*, vol. 10, pp. 42-55, 2013.
- [13] G. Deak, K. Curran, and J. Condell, "A survey of active and passive indoor localisation systems," *Computer Communications*, vol. 35, pp. 1939-1954, 2012.
- [14] P. Tsang, C. Wu, W. Ip, G. Ho, and Y. Tse, "A Bluetooth-based Indoor Positioning System: A Simple and Rapid Approach," *Annual Journal IIE (HK)*, vol. 35, pp. 11-26, 2015.
- [15] B. Yu, L. Xu, and Y. Li, "Bluetooth Low Energy (BLE) based mobile electrocardiogram monitoring system," in *Information and Automation (ICIA), 2012 International Conference on*, 2012, pp. 763-767.
- [16] X. Zhu, S. K. Mukhopadhyay, and H. Kurata, "A review of RFID technology and its managerial applications in different industries," *Journal of Engineering and Technology Management*, vol. 29, pp. 152-167, 2012.
- [17] B. Wang, M. Toobaie, R. Danskin, T. Ngarmnil, L. Pham, and H. Pham, "Evaluation of RFID and Wi-Fi technologies for RTLS applications in Healthcare Centers," in *Technology Management in the IT-Driven Services (PICMET), 2013 Proceedings of PICMET'13*, 2013, pp. 2690-2703.
- [18] P. M. Reyes, S. Li, and J. K. Visich, "Assessing antecedents and outcomes of RFID implementation in health care," *International Journal of Production Economics*, vol. 136, pp. 137-150, 2012.
- [19] M. D'Aloia, F. Cortone, G. Cice, R. Russo, M. Rizzi, and A. Longo, "Improving energy efficiency in building system using a novel people localization system," in *Environmental, Energy, and Structural Monitoring Systems (EESMS), 2016 IEEE Workshop on*, 2016, pp. 1-6.
- [20] M. Bal, H. Xue, W. Shen, and H. Ghenniwa, "A 3-D indoor location tracking and visualization system based on wireless sensor networks," in *Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on*, 2010, pp. 1584-1590.
- [21] D. Zaim and M. Bellafkih, "Bluetooth Low Energy (BLE) based geomarketing system," in *Intelligent Systems: Theories and Applications (SITA), 2016 11th International Conference on*, 2016, pp. 1-6.
- [22] (2016, 25 May 2017). *Bluetooth Low Energy*. Available: <https://www.bluetooth.com/what-is-bluetooth-technology/how-it-works/low-energy>
- [23] G. Han, G. J. Klinker, D. Ostler, and A. Schneider, "Testing a proximity-based location tracking system with Bluetooth Low Energy tags for future use in the OR," in *E-health Networking, Application & Services (HealthCom), 2015 17th International Conference on*, 2015, pp. 17-21.
- [24] S. Raza, P. Misra, Z. He, and T. Voigt, "Building the Internet of Things with bluetooth smart," *Ad Hoc Networks*, 2016.
- [25] (2016, 25 May 2017). *Bluetooth 5*. Available: <https://www.bluetooth.com/what-is-bluetooth-technology/how-it-works/bluetooth5>
- [26] A. A. N. Shirehjini, A. Yassine, and S. Shirmohammadi, "Equipment location in hospitals using RFID-based positioning system," *IEEE Transactions on information technology in biomedicine*, vol. 16, pp. 1058-1069, 2012.
- [27] T. Adame, A. Bel, A. Carreras, J. Melià-Seguí, M. Oliver, and R. Pous, "CUIDATS: An RFID-WSN hybrid monitoring system for smart health care environments," *Future Generation Computer Systems*, 2016.
- [28] R. Faragher and R. Harle, "An analysis of the accuracy of bluetooth low energy for indoor positioning applications," in *Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2014), Tampa, FL, USA, 2014*, p. 2.
- [29] S. Ahmad, R. Lu, and M. Ziaullah, "Bluetooth an Optimal Solution for Personal Asset Tracking: A Comparison of Bluetooth, RFID and Miscellaneous Anti-lost Traking Technologies," *International Journal of u-and e-Service, Science and Technology*, vol. 8, pp. 179-188, 2015.
- [30] J.-S. Lee, M.-F. Dong, and Y.-H. Sun, "A preliminary study of low power wireless technologies: ZigBee and Bluetooth low energy," in *Industrial Electronics and Applications (ICIEA), 2015 IEEE 10th Conference on*, 2015, pp. 135-139.
- [31] B. Jachimczyk, D. Dziak, and W. J. Kulesza, "Using the Fingerprinting Method to Customize RTLS Based on the AoA Ranging Technique," *Sensors*, vol. 16, p. 876, 2016.

CHARIOT: An IoT Middleware for the Integration of Heterogeneous Entities in a Smart Urban Factory

Cem Akpolat¹, Doruk Sahinel¹, Fikret Sivrikaya¹, Grzegorz Lehmann², and Sahin Albayrak²

¹German-Turkish Advanced Research Center for ICT, Berlin, Germany

²DAI Labor, Technische Universität Berlin, Germany

Abstract— The main innovation behind Internet of Things (IoT) is the fact that numerous devices will be able to communicate with their surroundings and the world in general. This communication ability of devices is expected to transform the existing network infrastructure in a radical way. The massive growth of the number of connected devices with IoT and the diversity of IoT use-cases and services bring significant technical challenges to existing communication network infrastructures, as they need to integrate heterogeneous and networked devices, objects and services with different requirements. In order to overcome these issues and to realize the potential of IoT, we propose a middleware called CHARLOT, which devises a runtime environment integrating heterogeneous resource-constrained devices and sensors communicating with various protocols, and a scalable and dynamic communication layer that abstracts the connected devices and enables their intercommunication. An urban smart factory scenario is used to highlight the future IoT requirements and the need for CHARLOT.

Index Terms—IoT, Device Abstraction, Directory Service, Device Heterogeneity

I. INTRODUCTION

FOLLOWING the global interconnection of people and services through the Internet, the concept of Internet of Things (IoT) has been on the rise with the ambition to digitalize and interconnect everyday objects in many domains of life and work. The great potential of this ambition lies in the holistic networking of the involved entities, i.e., the ability of any device to interact with any other device. Services that are able to make use of device communication and the data they provide are likely to expand and offer novel opportunities in various domains such as industry, healthcare, vehicular traffic and entertainment. Nevertheless, the increasing number and variety of devices or sensors in the growing IoT world makes it ever more complex to realize and manage such holistic interconnection systems. Available IoT solutions are mostly developed either for small sized platforms or for specific scenarios with a predefined set of sensors or devices, and they are far from providing the dynamic scaling and adaptability required to realize the added value of IoT holistic networking.

Orchestrating seamless communication among heterogeneous devices is a typical challenge in the IoT domain, therefore it draws attention as an emerging research problem. In order to illustrate those challenges, we realize a *smart urban factory* testbed from Industry 4.0 (i40) domain with as many physical components as possible, without relying on heavy industry components. Smart urban factory is a future oriented

factory, in which various primitive and complex devices like cyber-physical systems (CPS), software entities, robots and humans work cooperatively to produce an individual product designed by its customers. The objective of smart urban factory is to virtualize the whole factory components by abstracting all devices and systems, and ensuring an interoperable communication environment for its users. As a result of this abstraction, customers will be able to monitor their product, while remaining agnostic to underlying devices and protocols.

CHARLOT project provides a scalable IoT middleware that highlights the holistic networking of IoT entities representing heterogeneous devices or services, and demonstrates its features through a smart urban factory environment where it shows, e.g., how smart things can be connected to each other in the production line process in cooperation with humans and robots, how the warehouse stores products, and how the products are delivered. All these challenging processes include various devices ranging from primitive to complex ones, and also human actors. In this paper, we propose a new approach for the communication layer in CHARLOT project to address the interoperability in heterogeneous environment to ensure a homogeneous and reliable communication among all virtualized entities representing various devices and software with distinct characteristics.

The rest of the paper is organized as follows: Section 2 discusses the general required criteria of IoT runtime environments (REs) that connect sensors and devices with different communication protocols to each other and the Internet, and compare them based on these criteria. Section 3 gives insight into the architecture of CHARLOT middleware, followed by the novel interoperable communication approach towards i40. In Section 4 we introduce the CHARLOT smart urban factory use case, after which we share our initial results about device abstraction in the runtime environment and future work in Section 5. Finally, we conclude the paper in Section 6.

II. BACKGROUND AND RELATED WORK

If an IoT platform targets a holistic interconnection system for services, devices and sensors, then it should be able to provide solutions for challenges such as heterogeneity, availability, interoperability and scalability, all of which are well-known in the IoT domain [1]. Availability of services and

devices either as software or hardware, and the trusted (non-modified) data availability at each layer of IoT must be guaranteed in such a platform. The increase in device heterogeneity necessitates not only interoperable communication among the heterogeneous devices, but also an abstraction of devices, so that the platform is agnostic to underlying devices and protocols. Life-cycle management of each service and device, including continuous monitoring, control and configuration, has to be carried out to maintain interoperability in such platforms. Finally, IoT platforms should also be designed in a scalable way, so that it is possible to add new devices and services without imposing a challenge on existing services while adapting itself to resource-constrained and resource-rich situations. For a detailed analysis of IoT platforms, the readers are encouraged to check [2].

IoT platforms are composed of many layers such as objects (device layer), object abstraction, service management, application layer and business layers [1], each of which plays a special role and performs specific tasks. The first interaction with devices occurs in the device layer, where the data are collected from attached sensors or devices and then are transmitted to the upper layers through IoT Runtime Environment (RE). IoT RE is an important component of CHARIOT, which should act as a bridge between IoT devices and the middleware. In this section, we identify available IoT REs that we believe are most suitable to CHARIOT middleware and evaluate their capabilities that should cover the following aspects: Modularity, scalability, i.e., the capability of running on a wide range of resource-constrained and non-resource constrained platforms, holistic view of the connected devices, full device abstraction and compatibility with common IoT communication protocols, unified API to access devices from IoT apps, openness, automatic app loads and updates, platform-independence, and access management to apps and devices.

Eclipse Kura [3] offers a general middleware and application container for IoT RE services. It provides a manageable and intelligent RE, on which running applications can aggregate data and share them securely with a cloud platform. IoT REs have a requirement of being able to run on any IoT device, and Kura fulfills this requirement to some extent by being able to run on various platforms such as mobile devices, desktop, wearables and Raspberry PI [2]. Kura is a Java-based platform built on top of the Open Service Gateway Initiative (OSGi) framework; therefore, it is compatible with Windows and Linux and other operating systems for which Java is available. To summarize, Kura can run on resource-constrained devices, but there is a limitation due to OSGi.

Kura offers many services for IoT devices. I/O services enable access to the underlying hardware, then the data collected from the hardware can be saved, forwarded and published at the IoT RE with data services. Kura enables direct communication with cloud platforms, and remote management feature of Kura makes it possible to manage IoT apps via MQTT protocol. Networking Service provides an API that possesses enhanced routing and networking capabilities to

abstract many communication technologies such as Ethernet, Wi-Fi, and cellular networks. Last but not least, Watchdog Service monitors critical components and undertakes failure detection. The main focus of the Kura project is to bind sensors and actuators, collect data and transfer it to the cloud. It cannot satisfy CHARIOT requirements mentioned in Section III, as it is not scalable enough, the development of a device driver is not well-documented and the provided interface for devices is not user-friendly.

Alljoyn [4] is one of the emerging frameworks in IoT domain and it offers an open source framework that provides interoperability among heterogeneous devices, execution of distributed applications and dynamic composition of proximal networks. Furthermore, Alljoyn's framework targets a standard communication in mobile P2P systems. Discovering proximal devices and applications, adapting the framework based on the device characteristics, providing many connectivity technologies such as Bluetooth and Wi-Fi, and ensuring interoperability between distinct operating systems are some of the prominent features of Alljoyn. That being said, Alljoyn has some limitations to be used in a holistic IoT platform design, such as not being scalable enough to manage large scale smart IoT objects, not being able to manage big data storage and real-time analytics, and no support for the connection of devices residing under different subnets, meaning that all devices should reside under the same local network. Furthermore, a central thing manager does not exist and all nodes should connect to each other, leading to a likely increase in delay and non-reliable communication.

IoTivity [5] is an open source project aiming to enable seamless and secure device-to-device (D2D) connectivity in IoT ecosystem that is mainly supported by Samsung and Intel. The core motivation behind the IoTivity project is to bring together the open source community to speed up the creation of new framework and services required to bind the IoT devices. Its architecture provides various communication mechanisms, ensures security and identity, defines object models and APIs, guarantees interoperability between devices and applications, and connects all possible devices ranging from simple wearables up to smart cars.

The framework model of IoTivity comprises of four essential blocks: discovery, data transmission, data management and device management. Multiple discovery mechanisms for devices and resources in proximity and remotely are supported. Information exchange and control messages rely on a messaging and streaming model. Aggregation, storage and analysis of data from devices are carried out to manage the data, and device configuration, provisioning and diagnostic of devices are handled via device management module. IoTivity offers two different environments, one for resource-constrained and another for resource-rich devices. It runs on various operating systems such as Android, Linux, Arduino, Tizen, and Windows.

IoTivity platform is designed as connectivity-agnostic with the aid of the abstraction of connectivity layer, i.e., it supports wired and wireless connection technologies such as

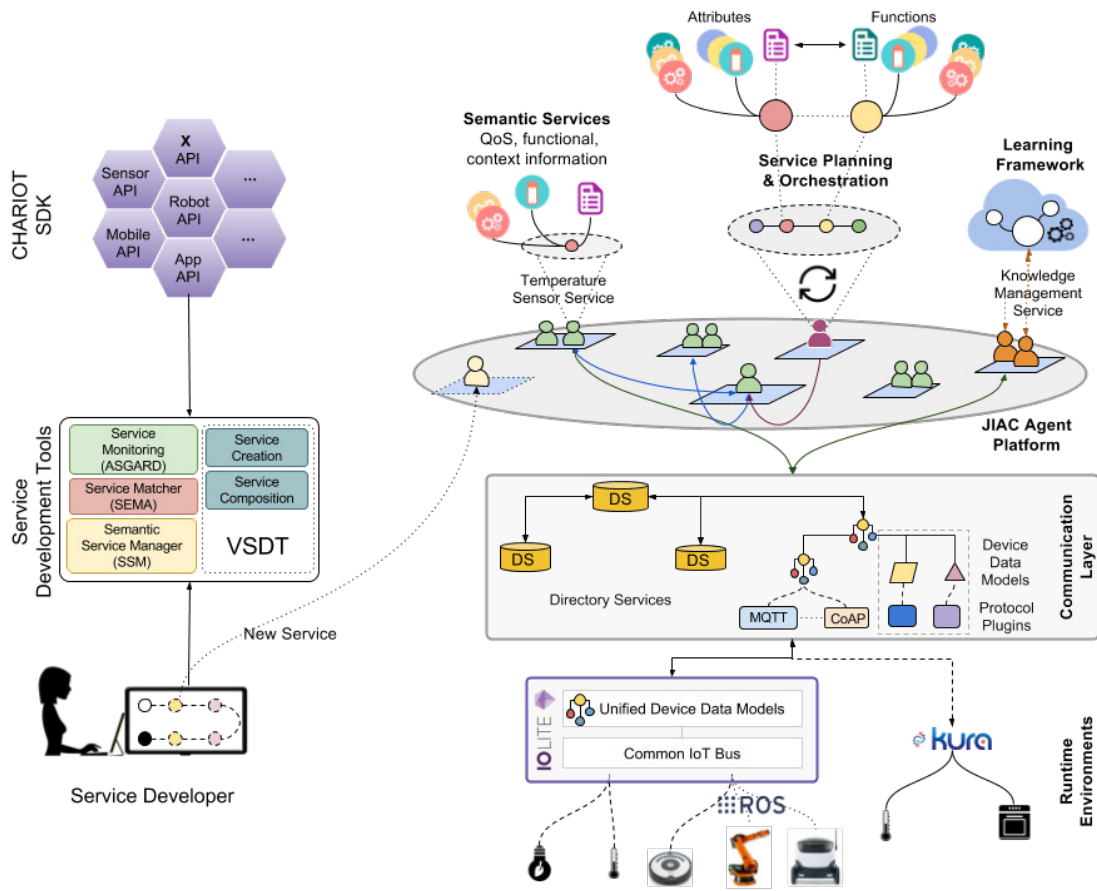


Figure 1: High-Level System Architecture of CHARIOT Middleware

Wi-Fi, Ethernet, Bluetooth-Low-Energy (BLE), Near-Field-Communication (NFC). Connectivity-agnostic layer of IoTivity makes it favorable in comparison to other platforms; however, it still does not conform to the desired CHARIOT middleware needs, as it only focuses on D2D communication and does not consider how an added value can be created from these interconnected devices via novel applications.

IOLITE is a Smart Home - Smart Building platform, providing the foundation for an open smart home ecosystem [6]. It offers the possibility to integrate devices of many kinds and to use them in a variety of applications in a wide variety of ways. IOLITE itself is a closed source environment but offers several APIs for extending the platform (i.e., an interface for developing apps to control the system as well as extension points for supplying new drivers for devices and sensors, if not already provided). The main features that characterize the IOLITE Platform are open SDKs for extension, offline capability, support for different user types, smartness, adaptivity, extensibility with new apps and drivers, and a customizable and modular structure.

Even though IOLITE is originally designed for smart home environment, its flexible architecture enables the integration of new custom devices, thus its usage area can be expanded

to other IoT domains. Furthermore, IOLITE abstracts all heterogeneous devices and represents them with a common device model in its ecosystem. Through this abstracted device model, CHARIOT middleware does not have to deal with the issues stemming from device heterogeneity. IOLITE RE differs from the other analyzed REs by providing a user-friendly platform, user management for devices that can enable access rights management, and an app-store that enables deploying many applications that can make use of the properties of the connected devices. Moreover, IOLITE provides a unified programming interface that makes the implementation of a driver and an application quite simple. Last but not least, the automatic update feature of IOLITE is seamlessly operated without touching any configuration file, once the new version is available.

III. CHARIOT ARCHITECTURE

CHARIOT offers an IoT middleware that encompasses many layers ranging from device layer to service layer. Device layer behaves as an IoT gateway for various devices that communicate with different protocols, and abstracts device features for other layers. The communication layer provides reliable communication for the services that represent devices, and enables device querying through their semantic

service descriptions. These descriptions are recognized by the semantic service layer of CHARIOT. The management and orchestration of semantic services is carried out by the service planning and orchestration component. This component offers context- and location-aware and error-resistant planning for operations by continuously monitoring QoS parameters of services and by reacting to the dynamic changes that occur, for instance, in case of a service-chain crash. This highly dynamic environment requires autonomous and adaptive behaviors for services, which is provided in CHARIOT by the knowledge management layer. Knowledge management layer adds learning capability to services and makes it possible to transfer the obtained knowledge among the services. The protection of those services and their access to the devices are carried out by the security layer that manages the access control mechanism.

To improve the ease of use for an IoT platform, an extendible platform is required in addition to the above mentioned constructive layers. CHARIOT middleware provides an SDK that facilitates the integration of any device ranging from primitive to sophisticated device, software entities to human actors, and a number of software development tools that deal with the monitoring, maintenance and control of those services. All these layers and tools are designed on top of an agent platform that forms a distributed service structure. The architecture of CHARIOT, which covers all layers and tools, is presented in Figure 1.

As mentioned above, one of the essential goals of CHARIOT is to highlight the holistic networking of IoT entities representing devices or services on the platform with device-heterogeneity support and ensure their continuous availability. In this study, we focus on the RE and communication layer of CHARIOT middleware, where device heterogeneity and scalability are ensured.

A. Runtime Environment

CHARIOT uses IOLITE as an RE to interact with IoT devices, as mentioned in Section 2. In this section, we explain how device integration into CHARIOT middleware is achieved by using IOLITE. The integration of devices over IOLITE in CHARIOT middleware requires two steps from the device layer perspective. First, the device drivers implemented for IOLITE are integrated and then the integration of IOLITE RE to CHARIOT middleware via Message Bus Protocol is carried out as described below:

1) *Device Driver Development and Integration:* The realization of smart factory use case scenario requires the development of a number of special drivers for sensors and actuators. During the driver development phase, first the feature of the devices and the supported communication protocols are identified. As the communication protocol varies from device to device, i) RE should be capable of extending itself to support different communication protocols such as Wi-Fi, BLE, Zigbee. ii) The data transmission between device and RE has to be solved by supporting different data transmission protocols like CoAP, MQTT, REST, SNMP, ModBus, TCP, UDP. iii) Through the established communication and data

transmission in XML, JSON or another format between RE and device, device functionalities can be mapped to RE device model concept, thus abstracting it for the upper layers.

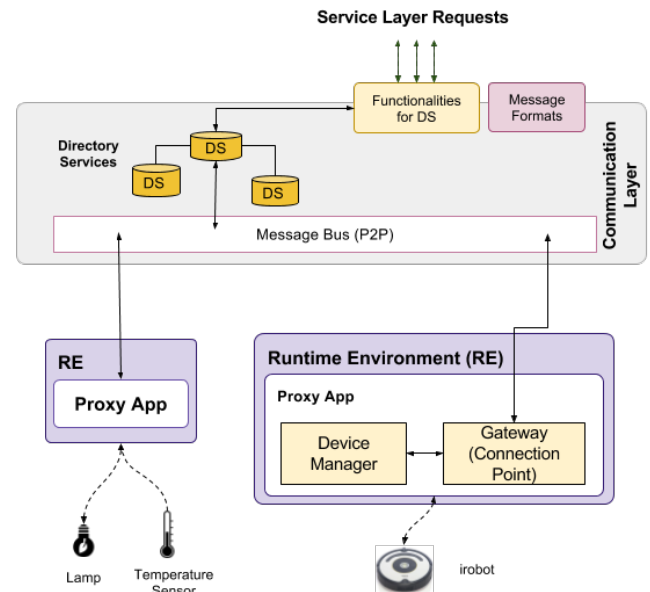


Figure 2: Integration of RE to Chariot Communication Layer

2) *Integration to CHARIOT Middleware:* The future-oriented IoT middleware needs a system in which IoT devices represented by software entities should interact with each other to create new value-added services and apps. The creation of this interaction environment necessitates first the integration between REs and CHARIOT middleware to map the physical devices to their virtual entities. All these communication processes and seamless integration would be performed through Message Bus. To build a bridge between RE and CHARIOT middleware over the Message Bus, a proxy RE application, depicted in Figure 2, is required in order to initiate the communication to CHARIOT communication layer and later to transmit devices' data and their models. This initiation message should include RE identifier, its device identifier and device property identifiers. In case the value of device property is accessed, these three identifiers have to be provided to access the device with another message type, which will be defined in the system architecture.

The massive data generation from devices, their analysis and the extraction of valuable information to optimize the processes in the smart factory may overstretch the limits of CHARIOT cloud and it might be possible that the minimum latency required in certain smart factory scenarios cannot be guaranteed. To address this issue, the proxy RE app will transfer some service functionalities using fog computing approach [7] to the device layer, i.e., to the RE that serves as an IoT gateway, to decrease the latency and enable data processing at the edge without transmitting the data to the cloud. With the help of this approach, IoT RE itself would be responsible to

decide for the amount of data to be stored from the devices, the frequency of data updates, registration and removal of devices, etc. In case communication between two IoT-REs is needed, it can be established via P2P communication.

B. Ensuring Interoperability in Communication Layer

Communication layer in CHARIOT matches incoming service requests with relevant IoT entities, and it promises scalable communication between different REs to enable P2P links between IoT devices. Three different software modules are provided to CHARIOT developers in the communication layer, so that they can interconnect all high-layer services to low-layer devices and entities regardless of what communication protocols they use and the environment in which an application is developed.

- 1) **Message Format:** The first software library involves application independent formats for messages between the RE that the devices or their software units are registered and the directory service (DS). This messaging format is used for device registration, removal and status updates.
- 2) **Scalable Directory Service:** DS is responsible for providing information about devices that are connected to the CHARIOT middleware and for storing the relevant path that enables the communication with these devices and accessing their current status. Device information is stored as OWL-S descriptions [8].
- 3) **P2P Communication:** Another essential feature of the communication layer is establishing communication channel between entities connected to CHARIOT. For this reason, a software library is formed to cover P2P messaging and security related functionalities.

The communication components given above are pictorially represented in Figure 2. In the following subsections, we describe these components in more detail.

1) **Message Protocol Definition:** Messaging formats in the communication layer are specifically defined for the interactions between the RE and the DS. In CHARIOT architecture, the RE collects all the device information and then forwards this information to DS by using this messaging protocol. This messaging protocol should also be able to inform the DS about errors and unknown messages. The modules that are used between the RE and the DS for messaging is shown in Figure 3. A communication protocol library is constructed in CHARIOT to be used by a protocol adapter that provides interfaces for different messaging protocols such as MQTT and CoAP. The RE can choose an interface defined in this adapter to communicate with the DS. A new interface must be added to this library, should an RE choose to communicate via a new protocol. The content of the messages that reach the communication layer should be modeled by the RE beforehand, so that the message broker and analyzer in the communication layer can extract the data in these messages and forward them to the related domain within the DS.

2) **Distributed and Scalable Directory Service:** DS stores device information in a location and content identifier for information-centric networking (ICN), so that other

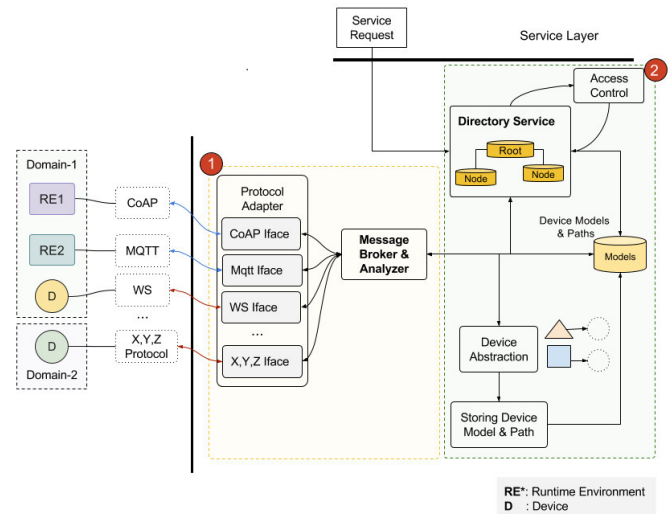


Figure 3: Communication Layer Architecture

devices in the device layer and the services that want to make use of the device can locate this device within the CHARIOT framework. The device description in the DS is taken from IOLITE Property Profile Model and converted to a URL-like address (e.g., *Inc://de.gt-arc.iot/sensor?lat=35,lon=11,radius=1km,scale=census*).

This device information is also used during end-to-end messaging between devices and their software agents. As all devices in CHARIOT are represented as software agents in the service layer and are defined with semantic OWL-S descriptions, semantic search can be used for finding devices and enabling end-to-end messaging. For this reason, DS has to enable messaging both in the device layer and in the service layer. As explained in the previous subsection, device layer messaging happens between the RE and the DS, and the content of the message includes device information stored in the DS. In addition, an agent in the service layer can query the DS to establish P2P communication with another device. Service layer to DS communication involves semantic search queries from the service layer to find the relevant device information. In our DS, Semantic Service Matcher (SeMa) [9] is responsible for finding structural, logical and semantic relation among services and returning search results for these queries.

A distributed DS design is considered in CHARIOT in order to meet the scalability and latency requirements and to provide an increased performance for the platform. The design consists of DS nodes that are distributed among different domains, such as a common property (e.g., energy consumption) or a common location (e.g., warehouse). All these DS nodes are connected in a hierarchical manner to a root DS that keeps track of the devices within the CHARIOT framework and is responsible for DS monitoring, synchronization and update tasks.

Root DS should be deployed as a cloud-based scalable entity

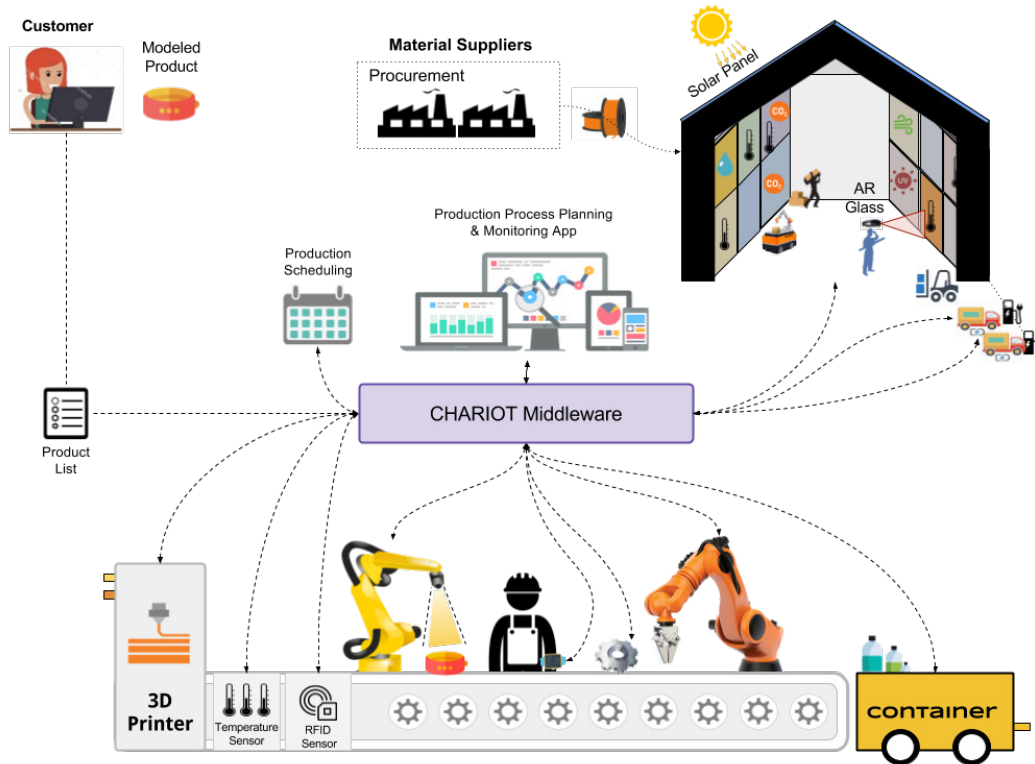


Figure 4: Industry 4.0 Urban Smart Factory Use Case

and should be able to distribute the load on a DS when required. In addition, data caching and sharing functions will be designed for the DS to increase the efficiency and to overcome response time constraint [10]. With all these functionalities, DS forms the backbone of the decentralized, hierarchical and scalable communication infrastructure of CHARIOT, which extends across multiple administrative domains.

An ICN-based architecture is foreseen for the DS design in CHARIOT. In such an architecture, DS nodes serve as ICN routers, where data packets are routed based on their contents in order to match service requests to suitable IoT devices or vice versa [11]. DS nodes can also cache information to speed up querying and data transmission in general. The main advantage of an ICN-based DS structure is its built-in content-based search and caching functions, which is very helpful for service discovery from the service layer. Device registration can either occur at the closest directory node or at the root directory node and then the root directory chooses the most suitable storage node for the device based on the device description.

3) *P2P Communication*: P2P communication can take place as the underlying data exchange for agent-to-agent communication in the service layer, or as direct communication between devices that require data from other devices at the device layer. In the first case, two agents communicate via ActiveMQ protocol at the service layer after searching for

the matching service description in the DS. In the second case, the communication layer is only responsible for data exchange between two REs, as the data passes through the Message Bus. Once the message reaches the RE, communication from the RE to the device is handled internally by the RE. The essential role of this component is to ensure a secured communication channel (Message Bus) between RE and CHARIOT middleware with SSL/TLS or another secure method, while DS is in charge of providing registered device addresses to REs. In addition, the interaction between IoT devices running on different REs (RE-to-RE communication) via P2P communication in a common message format should be defined to provide seamless interaction between devices.

IV. SMART URBAN FACTORY USE CASE FOR CHARIOT

Industry 4.0 introduces a new manufacturing perspective that uses new technologies and devices that can autonomously communicate and exchange data among each other. In a smart urban factory model, where the decisions are taken in a decentralized fashion thanks to autonomous systems, virtualized copies of physical devices and processes are monitored by more complicated computers, fulfilling almost all requirements of i40. As i40 has a direct relation to Cyber-Physical Systems (CPS), IoT and cloud computing, its improvement is also indispensable, even though it is in the early stages of its development. Moreover, increasing device heterogeneity and their varying requirements (e.g., CPU, bandwidth, memory),

the enhancement in analytic functionalities that enable better estimation on the device layer, and generation of efficient business applications with human-machine integration would foster the developments in i40. In the following, we introduce a use case scenario that brings mass customization, 3D printing, predictive maintenance, human-robot interaction, warehousing and augmented reality features together to demonstrate a smart urban factory environment and show how our approach aids in solving its challenges.

In a smart urban factory, we highlight the mass customization [12] feature of i40 and how other i40 features are harmonized with each other. The main idea of the mass customization is to construct a smart factory, as illustrated in Figure 4, which allows customers to create individualized products in any material and form. Customers may have the opportunity to produce a variety of products, ranging from bracelets to certain spare parts required for a machine. Customers use an online drawing platform that enables 3D modeling of the product design, which is then uploaded to CHARIOT middleware. CHARIOT schedules the printing time of the product models by taking many parameters such as priority, 3D printer and cartridge material availability, and energy consumption into account. These parameters' data are retrieved from all devices in the smart factory through REs and then unified in CHARIOT communication layer. The scheduled product models with a unique identifier are printed in 3D printers and on a passive RFID chip containing ID and additional production information. 3D printer receives the printing order from printing service, which can directly access the 3D printers and their functionalities over RE. Once this process is completed, RFID reader helps direct the product to the corresponding conveyor belt. Before boxing the product, an inspection process through the camera should be performed to detect whether the product meets the requirements of the customer design. This process requires object recognition and image processing operations, for which the inspection camera establishes a communication over its RE and communication layer with a service in CHARIOT middleware that enables data processing either in the local or in the cloud. After a successful inspection, the product is taken either by a robot or human worker from the conveyor belt either to be delivered to the delivery truck or to be stored in the warehouse. In the warehouse, the products are stored and preserved with respect to their characteristics by using different sensor technologies such as temperature and humidity control. A continuous data aggregation through warehouse's REs and CHARIOT communication layer is performed as well, and then all data are processed in the CHARIOT middleware to react to any change or an abnormal behavior of the warehouse's sensors or actuators, such as sensor replacement or repair.

V. INITIAL RESULTS & FUTURE WORK

CHARIOT communication layer has two main tasks, namely, device abstraction and enabling communication between all devices connected to CHARIOT middleware. The first phase of the project focuses on the device abstraction

and in this section we present our initial work conducted in this phase thus far.

Device abstraction phase involves two steps: *i)* modeling a device and its features using *Profile Property Identifier (PPI)* and matching the device functions to the PPI, *ii)* transmitting the abstracted device data via proxy application to the communication layer. For the initial task, we modeled and implemented many devices such as charging station, solar panel, gate, parking sensor, motion sensor, smart meter using IOLITE SDK and PPI. We are now able to abstract devices using *IOLITE Device API* that returns a JSON device data model along with its current values. The implemented devices are depicted in Figure 5. In the second step, we design an IOLITE application that can transmit the device data model to the requester and receive requests from the communication layer or from other devices to execute the functions of connected devices using P2P communication.

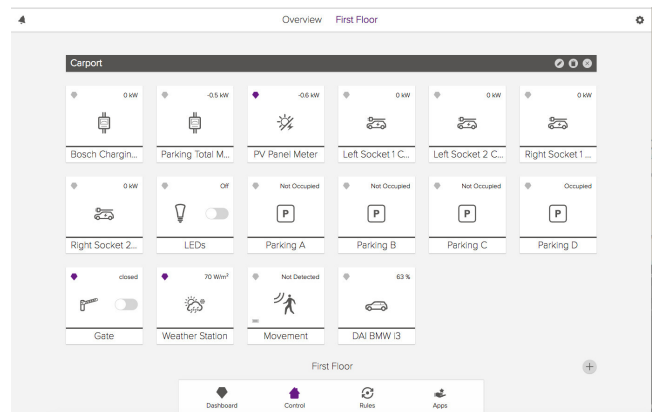


Figure 5: IOLITE Device Control Panel and Representation of Devices

This work mainly focuses on the CHARIOT communication layer; however, there are also other important cornerstones that play a crucial role in realizing the IoT middleware. For instance, the representation of devices as a service on JIAC agent-platform [13], the enrichment of services with semantic descriptions, the planning and orchestration of services and a learning engine that provides learning capability and knowledge sharing to services are among the ongoing and planned activities of the CHARIOT project. Furthermore, the project will provide software developers a CHARIOT SDK and a set of service development tools, which facilitate the creation, maintenance and monitoring of services.

VI. CONCLUSION

The emerging IoT devices and their increasing variety necessitate an interoperable communication layer in IoT domains. In CHARIOT project, we reflect the device heterogeneity through a smart urban factory use case. To strengthen our approach, we analyzed available IoT REs that are responsible for device connections, and justified the selection of IOLITE as RE. Then, the identified requirements of Industry 4.0

regarding smart urban factory use case are studied. To meet the identified requirements, we proposed CHARIOT device-agnostic communication layer, in which heterogeneous devices are abstracted in cooperation with the device layer. We shared our initial results, where we abstract devices through IOLITE RE, and we finally discussed our planned activities.

ACKNOWLEDGMENT

The work of authors at GT-ARC is supported in part by the German Federal Ministry of Education and Research (BMBF) under the grant number 01IS16045.

REFERENCES

- [1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2347–2376, 10 2015, doi:10.1109/COMST.2015.2444095.
- [2] M. A. Razaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 70–95, Feb 2016, doi:10.1109/JIOT.2015.2498900.
- [3] "Eclipse Kura," <http://eclipse.github.io/kura/doc/intro.html> (accessed: 2017-05-29).
- [4] M. Villari, A. Celesti, M. Fazio, and A. Puliafito, "Alljoyn lambda: An architecture for the management of smart environments in iot," in *2014 International Conference on Smart Computing Workshops*, Nov 2014, pp. 9–14, doi:10.1109/SMARTCOMP-W.2014.7046676.
- [5] J. C. Lee, J. H. Jeon, and S. H. Kim, "Design and implementation of healthcare resource model on iotivity platform," in *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, Oct 2016, pp. 887–891, doi:10.1109/ICTC.2016.7763322.
- [6] "IOLITE," www.iolite.de (accessed: 2017-05-29).
- [7] M. S. D. Brito, S. Hoque, R. Steinke, and A. Willner, "Towards programmable fog nodes in smart factories," in *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W)*, Sept 2016, pp. 236–241, doi:10.1109/FAS-W.2016.57.
- [8] "OWL-S: Semantic Markup for Web Services," <https://www.w3.org/Submission/OWL-S/> (accessed: 2017-06-19).
- [9] J. Fahndrich, T. Küster, and N. Masuch, "Semantic service management and orchestration for adaptive and evolving processes," *International Journal on Advances in Internet Technology*, vol. 9, no. 3&4, pp. 75–88, 2016.
- [10] J. Jung, E. Sit, H. Balakrishnan, and R. Morris, "Dns performance and the effectiveness of caching," *IEEE/ACM Transactions on Networking*, vol. 10, no. 5, pp. 589–603, Oct 2002, doi:10.1109/TNET.2002.803905.
- [11] I. Abdullahi, S. Arif, and S. Hassan, "Survey on caching approaches in information centric networking," *Journal of Network and Computer Applications*, vol. 56, pp. 48 – 59, 2015, doi:10.1016/j.jnca.2015.06.011. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1084804515001381>
- [12] F. S. Fogliatto, G. J. da Silveira, and D. Borenstein, "The mass customization decade: An updated review of the literature," *International Journal of Production Economics*, vol. 138, no. 1, pp. 14 – 25, 2012, doi:10.1016/j.ijpe.2012.03.002. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0925527312000989>
- [13] "Java-based Intelligent Agent Componentware," <http://www.jiac.de/agent-frameworks/jiac-v/> (accessed: 2017-05-29).

6th International Conference on Wireless Sensor Networks

A FEW years ago, the applications of WSN were rather an interesting example than a powerful technology. Nowadays, this technology attracts still more and more scientific audience. Theoretical works from the past, where WSN principles were investigated, grew into attention-grabbing applications practically integrated by this time in a real life. It could be said, that countless application fields, from military to healthcare, are already covered by WSN. Together with this technology expansion, still new and new tasks and interesting problems are arising. Simultaneously, such application actions stimulate the progress of WSN theory that at the same time unlocks new application possibilities. The typical examples are developments within the “Internet-of-Things” field as well as advancements in eHealth domain with WBAN IEEE 802.15.6 standard progress.

TOPICS

Original contributions, not currently under review to another journal or conference, are solicited in relevant areas including, but not limited to, the following:

Development of sensor nodes and networks

- Sensor Circuits and Sensor devices – HW
- Applications and Programming of Sensor Network – SW
- Architectures, Protocols and Algorithms of Sensor Network
- Modeling and Simulation of WSN behavior
- Operating systems

Problems dealt in the process of WSN development

- Distributed data processing
- Communication/Standardization of communication protocols
- Time synchronization of sensor network components
- Distribution and auto-localization of sensor network components
- WSN life-time/energy requirements/energy harvesting
- Reliability, Services, QoS and Fault Tolerance in Sensor Networks
- Security and Monitoring of Sensor Networks
- Legal and ethical aspects related to the integration of sensor networks

Applications of WSN

- Military
- Health-care
- Environment monitoring
- Transportation & Infrastructure
- Precision agriculture

- Industry application
- Security systems and Surveillance
- Home automation
- Entertainment – integration of WSN into the social networks
- Other interesting applications

SECTION EDITORS

- **Hodoň, Michal**, University of Žilina, Slovakia
- **Kapitulík, Ján**, University of Žilina, Slovakia
- **Kochláň, Michal**, University of Žilina, Slovakia
- **Micek, Juraj**, University of Žilina, Slovakia
- **Ševčík, Peter**, University of Žilina, Slovakia

REVIEWERS

- **Al-Anbuky, Adnan**, Auckland University of Technology, New Zealand
- **Baranov, Alexander**, Russian State University of Aviation Technology, Russia
- **Brida, Peter**, University of Zilina, Slovakia
- **Dadarlat, Vasile-Teodor**, Univiversita Tehnica Cluj-Napoca, Romania
- **Diviš, Zdenek**, VŠB-TU Ostrava, Czech Republic
- **Elmahdy, Hesham N.**, Cairo University, Egypt
- **Fortino, Giancarlo**, Università della Calabria
- **Fouchal, Hacene**, University of Reims Champagne-Ardenne, France
- **Furtak, Janusz**, Military University of Technology, Poland
- **Giusti, Alessandro**, CyRIC - Cyprus Research and Innovation Center, Cyprus
- **Grzenda, Maciej**, Orange Labs Poland and Warsaw University of Technology, Poland
- **Gu, Yu**, National Institute of Informatics, Japan
- **Hudík, Martin**, University of Zilina
- **Husár, Peter**, Technische Universität Ilmenau, Germany
- **Jin, Jiong**, Swinburne University of Technology, Australia
- **Jurecka, Matus**, University of Žilina, Slovakia
- **Kafetzoglou, Stella**, National Technical University of Athens, Greece
- **Karastoyanov, Dimitar**, Bulgarian Academy of Sciences, Bulgaria
- **Karpiš, Ondrej**, University of Žilina, Slovakia
- **Laqua, Daniel**, Technische Universität Ilmenau, Germany
- **Milanová, Jana**, University of Žilina, Slovakia

- **Monov, Vladimir V.**, Bulgarian Academy of Sciences, Bulgaria
- **Ohashi, Masayoshi**, Advanced Telecommunications Research Institute International / Fukuoka University, Japan
- **Papaj, Jan**, Technical university of Košice, Slovakia
- **Ramadan, Rabie**, Cairo University, Egypt
- **Scholz, Bernhard**, The University of Sydney, Australia
- **Shaaban, Eman**, Ain-Shams university, Egypt
- **Shu, Lei**, Guangdong University of Petrochemical Technology, China
- **Smirnov, Alexander**, Linux-WSN, Linux Based Wireless Sensor Networks, Russia
- **Staub, Thomas**, Data Fusion Research Center (DFRC) AG, Switzerland
- **Teslyuk, Vasyl**, Lviv Polytechnic National University, Ukraine
- **Wang, Zhonglei**, Karlsruhe Institute of Technology, Germany
- **Xiao, Yang**, The University of Alabama, United States

Analysis of the new modulation and coding techniques for VDSL

Ing. Tomáš Pajda,
 IEEE,
 Information Theory Society
 ul. Fučíkova 612/4,
 Poltár, Slovakia
 Email:
 ing.tomas.pajda@gmail.com

doc. Ing. Rastislav Róka, PhD.
 Slovak University of Technology,
 Institute of Multimedia
 Information and Communication
 Technologies, Ilkovičova 3
 Bratislava, email:
 rastislav.roka@stuba.sk

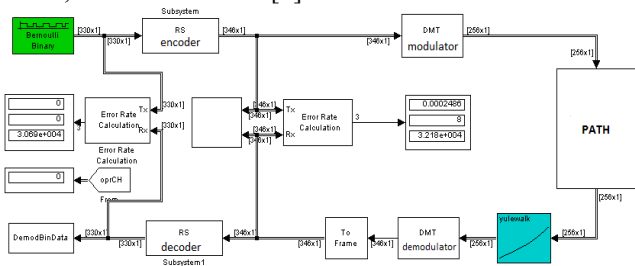
Abstract—Nowadays, the demand on higher transmission speed increased, because of more users using the Internet and the applications are demanding the higher transmission speed, too. In this article, we would like to give you our vision on increasing the transmission speed in VDSL technology.

I. INTRODUCTION

THE motivation to write this article was based on positive results from our testing in Matlab. We tried to overload the measured channel capacity. The overloading was made in terms of sending more modulation symbols than the SNR measurement provided for certain distance. We used two model situations. Let's assume, that we have two results of channel capacity for the distance 400 m. One result was for modulator settings for 300 m, where we could put more modulation symbols, because the signal-to-noise ratio was higher and we could get into the distance 400 m by using the Reed-Solomon codes and correct the errors, that happened during the transmission, because of lower signal to noise ratio in the distance 400 m than in the distance 300 m. In this case, we used virtually higher capacity of the transmission channel, for the distance 400 m (capacity was used from the distance 300 m). The result was that more transmission errors occurred. We thought, if it was possible to correct these errors using Reed-Solomon codes. Below is the description of our analysis.

II. ANALYSIS

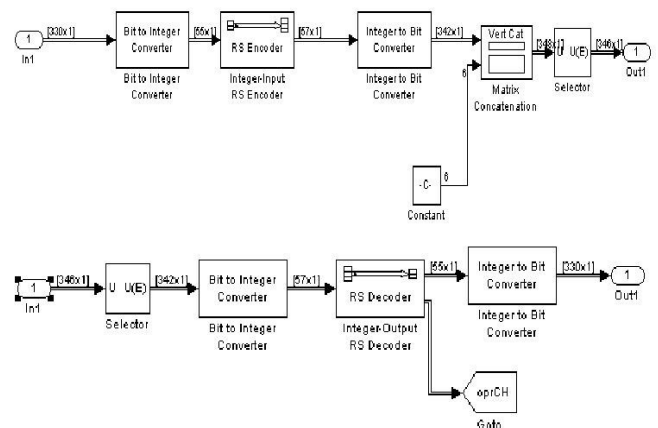
For the purpose of analysis, we used the communication model, created in Matlab [2].



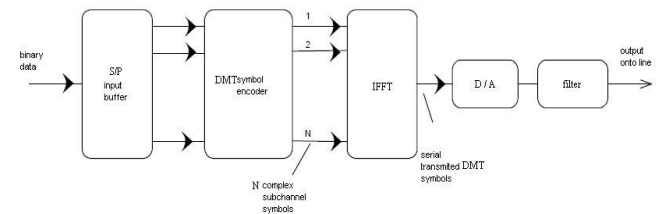
Picture 1. Simulation model

The simulation model was composed of the Bernoulli binary generator as a source of data, Reed-Solomon encoder, DMT modulator, transmission path with errors simulation, DMT demodulator, Reed-Solomon decoder and receiver of the transmitted data. There were two error counters, the first one was for modulation errors and the second one was for errors after application of Reed-Solomon codes.

First of all, we measured the capacity of the channel, without the Reed-Solomon codes, for the distances 300m, 400m, 500m, and 600m. In the case of errors in certain distance, we made another measurement, to accommodate the modulator to get errorless capacity and so transmission speed in each measured distance.



Picture 2.: Reed-Solomon encoder, decoder



Picture 3.: DMT modulator

After measurements, we had the number of modulation symbols N , that could be transmitted in the certain period of time, for each distance, for which the measurements were

made. The N parameter was then used as a length of the codeword for Reed-Solomon codes. Assuming the equation for FEC and capacity of the channel, that was:

$$K/N < C \quad (1),$$

where N was the number of the modulation symbols (and a length of the codeword as well), K was the amount of the useful information and C was the channel capacity. Because

$$N=K+2*T \quad (1.1),$$

And the N parameter was set by the measurement of the channel capacity, we had two parameters to vary with (K and T). The equation (1) can be also written in this way:

$$K/(K+2*T) < C \quad (2),$$

From this equation number 2, we can say, that if we want to transmit more data, that the parameter K represents, we must increase the T value, that represents the number of errors per frame, that the Reed-Solomon codes should be able to correct. So, if we want to increase the amount of the data K to be transmitted through the channel with the capacity C, we should increase the T parameter value. If we set the C value for 300 m and the real distance is 400 m, we should be able to correct more errors, but the result is higher transmission speed, even if more errors occurred during the transmission, because we can correct these errors by using the Reed-Solomon codes and the amount of data used for the parity of FEC is less than the gain of data in bits that we obtained by application of more modulation symbols transmitted per the unit of time, and Reed-Solomon codes. If we use higher channel capacity (can be achieved also by moving SNR function curve upper than measured) than measured, let's say

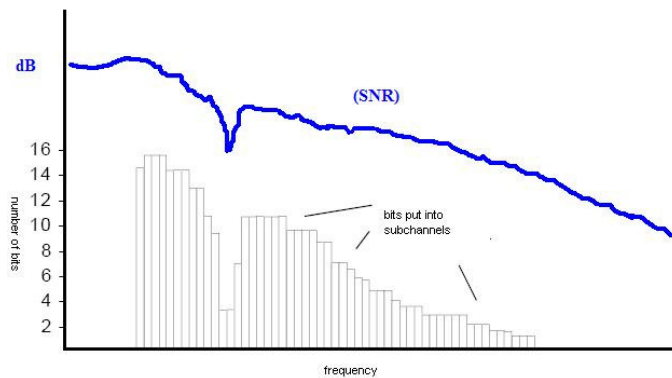
in 400 m if we use the capacity for 300 m, the N parameter will be higher, what means, that:

$$K / (K+2*T) \quad (3),$$

where

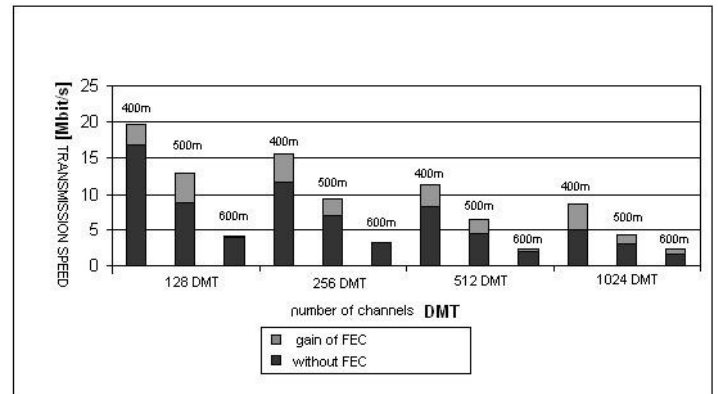
$$K+2*T=N \quad (4),$$

the K parameter can be higher, so the amount of the useful data can be increased, so the transmission speed will be higher. If we no keep the settings (N ,K) for the channel capacity measured for 300 m and apply it for the distance of 400 m, we will have to accommodate the T parameter according to the equation number (2).



Picture 4.: Signal-To-Noise Ratio

From the signal-to-noise ratio and measurement of the channel capacity in bits/s, we can find out the number of transmittable symbols, what is the codeword length as a parameter for the Reed-Solomon codes. Because of the characteristics of the metallic lines, used in DSL, the signal-to-noise ratio with increasing the distance, decreases, because of the influence of the metallic lines distortions. So, if we want to increase the transmission speed in longer distance, we should use the Reed-Solomon codes and so we can afford to use higher channel capacity than the metallic lines in required distance can provide us. Reed-Solomon codes are well behaving, because they can locate and correct the errors that occur during the transmission. Below, we will prove, that even if more parity bits are necessary to correct more errors when the channel capacity is overloaded (in the distance of 400 m we used settings of modulation for 300 m), we will still get gain in the terms of transmission speed.



Picture 5.: The results of testing

The picture number 5 shows us the results from the testing of the previous assumptions. Because of positive results, we wanted to define what was happening and wanted to understand, why we can get this gain in the transmission speed. From the results, we can say, that there is some gain visible. Next question is, whether the gain versus the parity length is still providing the gain in terms of more user data to be transmitted. We made an analysis from the table below (obtained from the measurement in Matlab made in [3]),

l	N	K	bit/symbol	RSoprCH	frVST	frM	RpM	RpC	errM	errC	sum[snr]	max[snr]	mean[snr]
[m]			[symbol]	[symbol]	[bit]	[bit]	[Mbit/s]	[Mbit/s]	[bit]	[bit]	[10*6dB]	[dB]	[dB]
300	51	49	6	1	294	311	24.88	23.52	12	0	23.55	51.13	16.83
325	51	49	6	1	294	311	24.88	23.52	19	0	20.36	49.55	15.91
350	51	49	6	1	294	311	24.88	23.52	47	11	18.76	47.99	14.65
350	51	49	6	4	258	311	24.48	20.64	51	0	18.16	47.47	14.19
350	46	44	6	1	264	278	22.24	21.12	27	3	17.55	47.14	13.71
350	46	40	6	3	240	278	22.24	19.2	18	0	18.36	47.28	14.34
375	46	40	6	3	240	278	22.24	19.2	61	0	16.44	45.99	12.84
400	46	40	6	3	240	278	22.24	19.2	142	0	14.25	44.71	11.14
425	46	40	6	3	240	278	22.24	19.2	332	13	11.79	43.43	9.21
425	46	36	6	5	216	278	22.24	17.28	323	0	10.11	42.96	7.5
425	36	30	6	3	180	217	17.36	14.4	90	0	10.01	43.7	7.82
450	36	28	6	4	168	217	17.36	13.44	260	0	8.34	41.85	6.51
450	32	26	6	3	156	157	15.76	12.48	150	0	6.29	42.16	4.91
475	32	24	6	4	144	157	15.76	11.52	317	0	5.11	30.98	2.43
475	30	26	5	2	150	151	12.08	10.4	24	0	1.42	40.72	1.11
500	30	26	5	2	150	151	12.08	10.4	95	0	0.82	39.48	0.64
500	27	23	5	2	115	136	10.88	9.2	45	0	-1.29	35.41	-1.01

Tab.: 1. Results of testing

where we put the gain in the transmission speed in bits on one side and the amount of data used for parity of FEC on the other side. Let's say that the gain for 350m was 20,64 Mbits/s – 19,2 Mbits/s, what equals to 1,44 Mbits/s. One more parity symbol was used, and if each parity symbol in this case means 6 bits, $1*6$ is 6 more bits to transmit. If we subtract 1,44 Mbits/s – 6 bits/s, the result is 1,44 Mbits/s. This means, that even if more parity symbols were used to get into longer distance errorless, we still will get the gain in terms of percentage, here $1,44 / 19,2$, what equals to cca 7,52 % of gain. From the results we can say that even if more errors occurred when the channel was overloaded in terms of more symbols transmitted in a unit of time, if we correctly set the Reed-Solomon codes, we will be able to repair the errors that occur during the transmission and because the error count is not increasing faster than the Reed-Solomon possibility to correct it, these codes are a good choice for increasing the transmission speed in VDSL. Our next idea is also to try to define the maximum of the channel overloading to define the maximum speed that using of these codes can provide. Let's assume the limity:

$$\lim_{T \rightarrow \inf} (K / (K + 2*T)) < C \quad (5)$$

How K value can be changed when increasing the T parameter? We can say, that if T increases, there is a possibility to increase the K, which represents the amount of data, what is in terms of transmission speed positive. But we must keep in mind also the equation mentioned above $N = K + 2*T$. So, the upper limity of increasing the parameters K and T is defined by this equation (5). Another fact that follows these assumptions is that if we want to increase the transmission speed in longer distance, we must use the number of bits assigned to a frame from lower measured distance, or just use higher number of bits than assigned by modulator (for example using higher signal-to-noise ratio to assign the number of bits to a frame).

III. ADVANTAGES OF FEC

Reed-Solomon codes and the RM OSI model

From the RM OSI model perspective, the modem is working on the physical layer. There are two possibilities of implementing the Reed-Solomon codes. The first one is the implementation into the modem, where we can have modulation and FEC in one device. The second one is, that we can make a device called Reed-Solomon codec and use it on the customer's premises. The thing is, that the definition of Reed-Solomon codes parameters should be same on each side of the transmission, what means that the generating polynome must be the same, to be able to encode and DECODE the information transmitted through the channel.

Reed-Solomon codes and synchronisation

The problem, that was not solved yet, was the synchronisation of the FEC. Let's say, that two clients want

to communicate and both are using the modem with Reed-Solomon codes. First of all, there must be the same generating polynome for the codes on both sides. Second condition that must be accomplished is, that during the settings of the connection on both sides, all parameters must be set properly (parameter N, K, T) and the same on both sides. This can be done by setting some exchange of parameters at the beginning of the communication. This will be time consuming at the beginning, but can be useful in terms of modem settings to higher transmission speed.

Reed-Solomon codes versus agregation

Another benefit is, that using Reed-Solomon codes we can get higher transmission speed without the agregation of lines with lower speed together. And so, if we do agregate these lines with Reed-Solomon codes, we can get much more higher capacity and so transmission speed than with agregation and without Reed-Solomon codes. We can play with these settings to obtain as high speed as possible.

Reed-Solomon implementation

The possible implementation could be based on defining the Galois field from the channel capacity measurement. After the measurement we have defined the number of modulation symbols that can be transmitted in the transmission period of time per unit, so called modulation speed. Each combination of modulation symbols is a codeword of FEC. The number of symbols possible to transmit in a period of time is a multiplication of codeword length. So, if we use higher codeword length, let's say in the distance 350m if we use the codeword length appropriate for 300m, which is higher, we can get higher modulation speed, but with more errors. But if we use some portion of the codeword for correction of the transmission errors, so called parity of the FEC, we will get higher transmission speed in 350m, than if we use the modulation settings for 350m. So, there is a benefit of using the FEC, here the Reed-Solomon codes, in ability to increase the transmission speed and get better results than before.

IV. CONCLUSION

From the text above, we can say, that it is possible to increase the transmission speed by appropriate use of the FEC, in this case Reed-Solomon codes, to get into longer distance with higher transmission speed. This also means, that we can keep the existing infrastructure of metallic lines and using the mathematical methods we can get into longer distance with higher transmission speed as well as increasing the amount of data, that we are willing to transmit by increasing the N parameter over the measured value. One thing that is not defined yet is the maximum increase of the frame length parameter in each distance compared to measured value in this distance. This idea can be an issue for further research in this topic. We just wanted

to show, that there is a way how to increase the transmission speed using the mathematical methods.

V. REFERENCES

- [1] S. Dlháň, Analysis of coding and precoding techniques for VDSL technology in access network, May 2003,
- [2] M. Halás, Analysis of new modulation techniques for VDSL technology in access network, May 2003.,
- [3] T. Pajda, R. Róka, Analysis of the new modulation and coding techniques for technology VDSL, May 2009.

Information Technology for Management, Business & Society

IT4MBS is a FedCSIS conference area aiming at integrating and creating synergy between FedCSIS events that thematically subscribe to the disciplines of information technology and information systems. The IT4BMS area emphasizes the issues relevant to information technology and necessary for practical, everyday needs of business, other organizations and society at large. This area takes a sociotechnical view on information systems and relates also to ethical, social and political issues raised by information systems. Events that

constitute IT4BMS are:

- AITM'17—15th Conference on Advanced Information Technologies for Management
- ISM'17 - 12th Conference on Information Systems Management
- IT4L'17—5th Workshop on Information Technologies for Logistics
- KAM'17—23rd Conference on Knowledge Acquisition and Management

15th Conference on Advanced Information Technologies for Management

WE are pleased to invite you to participate in the 14th edition of Conference on “Advanced Information Technologies for Management AITM’17”. The main purpose of the conference is to provide a forum for researchers and practitioners to present and discuss the current issues of IT in business applications. There will be also the opportunity to demonstrate by the software houses and firms their solutions as well as achievements in management information systems.

TOPICS

- Concepts and methods of business informatics
- Business Process Management and Management Systems (BPM and BPMS)
- Management Information Systems (MIS)
- Enterprise information systems (ERP, CRM, SCM, etc.)
- Business Intelligence methods and tools
- Strategies and methodologies of IT implementation
- IT projects & IT projects management
- IT governance, efficiency and effectiveness
- Decision Support Systems and data mining
- Intelligence and mobile IT
- Cloud computing, SOA, Web services
- Agent-based systems
- Business-oriented ontologies, topic maps
- Knowledge-based and intelligent systems in management

SECTION EDITORS

- **Andres, Frederic**, National Institute of Informatics, Tokyo, Japan
- **Dudycz, Helena**, Wrocław University of Economics, Poland
- **Dyczkowski, Mirosław**, Wrocław University of Economics, Poland
- **Hunka, Frantisek**, University of Ostrava, Czech Republic
- **Korczak, Jerzy**, Wrocław University of Economics, Poland

REVIEWERS

- **Abramowicz, Witold**, Poznan University of Economics, Poland
- **Ahlemann, Frederik**, University of Duisburg-Essen, Germany
- **Atemezing, Ghislain**, Mondeca, Paris, France
- **Brown, Kenneth**, Communigram SA, France
- **Cortesi, Agostino**, Università Ca’ Foscari, Venezia, Italy
- **Czarnacka-Chrobot, Beata**, Warsaw School of Economics, Poland

- **De, Suparna**, University of Surrey, Guildford, United Kingdom
- **Dufourd, Jean-François**, University of Strasbourg, France
- **Franczyk, Bogdan**, University of Leipzig, Germany
- **Januszewski, Arkadiusz**, UTP University of Science and Technology in Bydgoszcz, Poland
- **Kannan, Rajkumar**, Bishop Heber College (Autonomous), Tiruchirappalli, India
- **Kersten, Grzegorz**, Concordia University, Montreal, Poland
- **Kowalczyk, Ryszard**, Swinburne University of Technology, Melbourne, Victoria, Australia
- **Kozak, Karol**, TUD, Germany
- **Leyh, Christian**, Technische Universität Dresden, Chair of Information Systems, esp. IS in Manufacturing and Commerce, Germany
- **Ligeza, Antoni**, AGH University of Science and Technology, Poland
- **Ludwig, André**, University of Leipzig, Germany
- **Magoni, Damien**, University of Bordeaux – LaBRI, France
- **Michalak, Krzysztof**, Wrocław University of Economics, Poland
- **Owoc, Mieczysław**, Wrocław University of Economics, Poland
- **Pankowska, Malgorzata**, University of Economics in Katowice, Poland
- **Pinto dos Santos, Jose Miguel**, AESE Business School Lisboa
- **Rot, Artur**, Wrocław University of Economics, Poland
- **Stanek, Stanisław**, General Tadeusz Kosciuszko Military Academy of Land Forces in Wrocław, Poland
- **Surma, Jerzy**, Warsaw School of Economics, Poland and University of Massachusetts Lowell, United States
- **Teufel, Stephanie**, University of Fribourg, Switzerland
- **Tsang, Edward**, University of Essex, United Kingdom
- **Wątróbski, Jarosław**, West Pomeranian University of Technology in Szczecin, Poland
- **Wendler, Tilo**, Hochschule für Technik und Wirtschaft Berlin
- **Wolski, Waldemar**, University of Szczecin, Poland
- **Zanni-Merk, Cecilia**, INSA de Rouen, France
- **Ziemia, Ewa**, University of Economics in Katowice, Poland

Identification of Business Relevant Features in Information

Jiri Matula, Jaroslav Zacek
University of Ostrava,
Faculty of Science, Dvorakova 7,
Ostrava 701 03, Czech Republic
Email: {jiri.matula,
jaroslav.zacek}@osu.cz

Abstract—The paper is devoted to the utilization of DEMO enterprise ontology (Design & Engineering Methodology for Organizations) for refactoring purposes in software development. The main contribution of the paper resides in presentation of the method which interconnects ontological models of business processes with information system features implementation. Also, it allows the evaluation of their relevancy for enterprise. In contrast to other methods based on best practices, the proposal uses ontological description of business processes defined upon the theory in DEMO methodology. This makes the proposal unique compared to other approaches. Moreover, it provides a clear differentiation of features which are important for performing tasks by employees in company.

I. INTRODUCTION

GENERALLY, information systems (IS) provide information for task execution of many entities living in enterprise. Nevertheless, development of information systems is very prone to errors and challenges during its whole lifecycle. As a company develops in time and changes its internal rules and roles, information systems may tend to get old and some features do not fit to company needs. This fact often leads to refactoring, whereas developers are not able to satisfy user requirements due to limitations of the current implemented solution.

There are many techniques adopted by agile approaches how to gather and define user requirements for refactoring of information systems. Rational Unified Process uses Use Cases and scenarios to control the development process to ensure that requirements are always in first place (Use Case-driven approach). This technique visualizes a relationship only between an actor and the system without any other context (e.g. transactions, non-functional requirements) and this technique fits well for bigger information systems. Requirements gathering process in current methodologies (Scrum, Kanban) still relies on a one-way confirmation and inherently cannot provide instant automated feedback during software development. These methodologies have only one kind of feedback – user acceptance testing, in most cases performed manually by testers. BDD (Behavior-Driven Development) technique allows to get automatic feedback

and works well with a declarative approach. Using a declarative approach to describe business contracts can be found in [7] and authors use finite automata theory to simplify a relationship between elements. In another paper, authors use XML as a data source and brings a new extension to Courteous Logic Programs [8]. There are also attempts to use a semantic driven approach for user requirements verification [11]. However, this approach lacks the necessary verification. Some research tries to define a link between data mining and business process management [9]. This paper specifically points to the fact that constraints are described by a declarative process model. Authors also state that is possible to discover this model based on event data. However, if all states are not presented on the model (typically if unknown information system is being built without best practices), the correct technique is still missing to determine all states in small and middle size systems. A fully ontological approach can be found in [10] to access generic data source. In comparison, the DEMO methodology utilizes theoretical foundations to describe business processes, which makes this approach unique compared to the above mentioned approaches because they are mostly based on best practices.

The combination of BDD technique and DEMO methodology allows to link ontological descriptions of business processes directly to production code with the possibility of testing automation in a continuous integration process. Interconnection of information system features and coordination or production acts makes possible to determine which features of the information system can be removed, newly implemented, or refactored according to ontological descriptions derived upon DEMO methodology. Thanks to this fact, a new method is presented. It identifies features of information systems which are important for the execution of coordination and production acts performed by employees in companies.

II. TRANSACTIONS IN DEMO METHODOLOGY

DEMO methodology [3] defines an organization as a composition of people (social individuals) that perform two kinds of acts – production and coordination acts. The result of successfully performing a production act is a

production fact. An example of a production fact may be that the package that has been delivered has been paid, or offered service has been accepted. All realization issues are fully abstracted out. Only the facts as such are relevant, not how they are achieved. The result of successfully performing a coordination act is a coordination fact. Examples of coordination acts are requesting and promising a production fact. Coordination and production acts and facts are arranged into a transaction pattern.

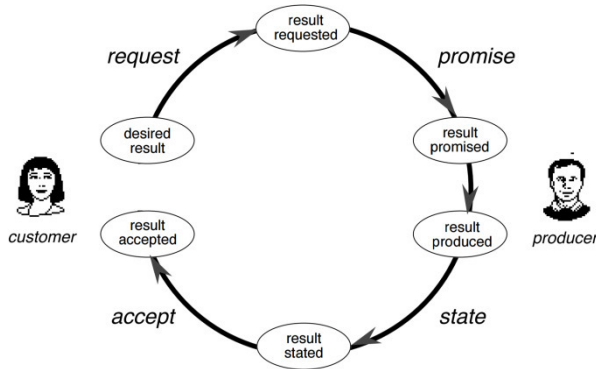


Fig. 1 Basic transaction pattern. Source: [3]

Transaction pattern states that there are always two roles in a transaction, initiator (customer) and executor (producer). Initiator is someone who has a request and executor is responsible for fulfilling initiator needs. More detailed explanation of transaction pattern is depicted in the Fig. 2. White rectangles represents coordination acts, white rounded rectangle is used for coordination fact. Production act is depicted as grey rectangle. Gray rounded rectangles stands for production fact. The lifespan of every transaction has three phases – order (proposition), execution and result

phase.

In the order phase, the initiator and the executor work to reach an agreement about the intended result of the transaction, i.e., the production fact that the executor is going to create as well as the intended time of creation. In the execution phase, this production fact is actually brought about by the executor. In the results phase, initiator accepts or rejects result (production fact) of the transaction [3].

According to DEMO methodology, it is possible to analyze gathered text descriptions of business processes of a company and extract transactions which represent ontological essence of the enterprise [6]. These transactions can be served as a source of information for revising features during refactoring process and they also form the theoretical basis which is implemented using BDD technique. Consequently, these specifications can be executed via DSL languages (Domain Specific Language) like Cucumber, Behat, etc.

III. CONVERSION OF TRANSACTIONS TO BDD SCENARIOS

The BDD technique which has been developed from the test-driven development technique utilizes principles of user stories and test-driven development approach [2]. User stories typically follow this recommended template.

As a <type of user>, I want <some goal> so that <some reason>.

Fig. 3 User story template. Source: [1]

At the same time, user stories technique is the foundation stone for the BDD testing scenario template, which is observable from a comparison of user story template above and BDD scenario template below.

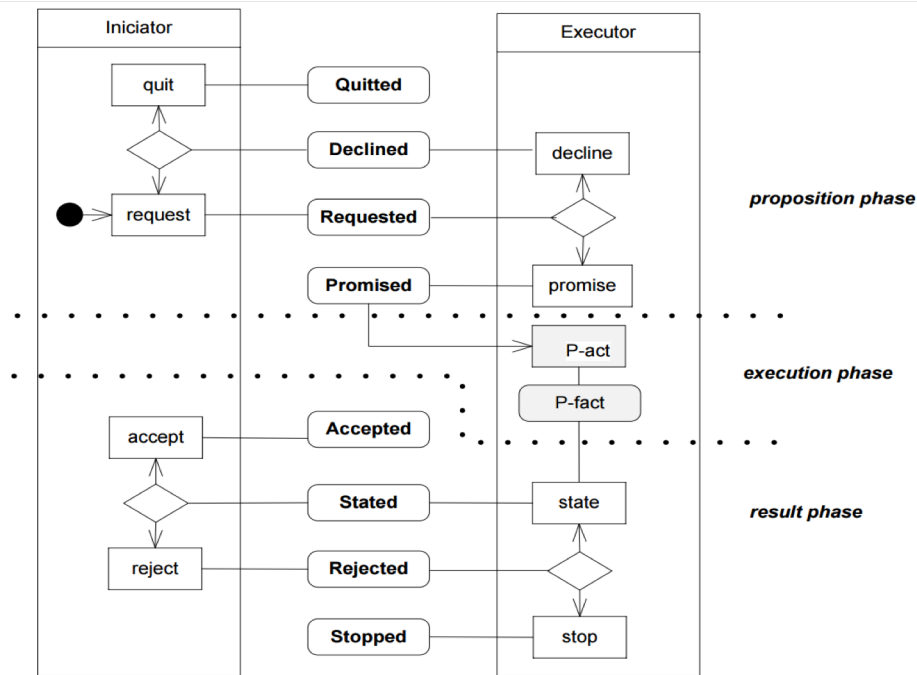


Fig. 2 Detailed view of transaction pattern. Source: [3]

Feature [title]
 In order to [benefit]
 As [role]
 I want [feature]
Scenario: [title]
 Given [context]
 And [some more context]
 ...
 When [an event occurs]
 And [a further event]
 ...
 Then [outcome]
 And [another outcome]
 ...
Scenario: [title]
 ...

Fig. 4 Standard BDD scenario template

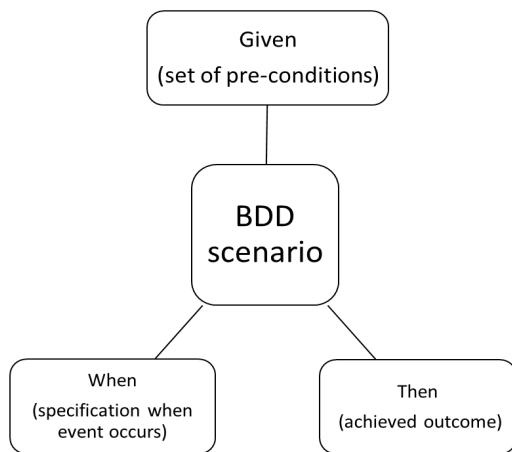


Fig. 5 Composition of BDD scenario

A previously mentioned fact is that user stories are part of BDD scenario template give an opportunity to apply modified version template into a BDD template scenario. In the context of user stories in the form of transactions, proposed modified version of template for BDD scenario looks as following.

As an <initiator/executor>, I perform a coordination/production act in <transaction> so that <result of transaction>.

Fig. 6 Modified template for user story. Adapted from: [4]

The role has been replaced for executor or initiator who takes a part in the transaction. Scenarios describe the business situation with the aim to fulfil business goals denoted as outcomes of transactions. All scenarios must respect user story given in the feature description.

Modified template structure starts with a feature title which is linked to related transaction unique ID. After feature identification, it is necessary to perform the next step – the outcome of the transaction – which is going to be

fulfilled when the transaction is completed. So far, context for coordination/production act is defined and follows a transformation text description of coordination or production act into the form of BDD scenarios. The scenario part should have covered all possible situations during the execution of the coordination/production act. All transformed coordination/production acts into BDD scenarios must have its reference in gathered text descriptions of business processes. Every coordination/production act must result in coordination/production fact.

Feature [title] – [transaction ID]
 In order to [coordination/production fact]
 As [initiator/executor]
 I want to perform coordination/production act in [transaction]
Scenario: [title]
 Given [context]
 And [another context]
 ...
 When [an event occurs]
 And [another event]
 ...
 Then [result – coordination/production fact]
 ...
Scenario: [title]
 ...

Fig. 7 Modified BDD scenario template. Adapted from: [5]

As an explanatory case is used a company where the messenger (executor) delivers packages to their customers. A company (initiator) usually comes with a request to perform a delivery. The initiator and executor performs coordination and production acts in order to deliver a package. These coordination and production acts are expressed in the scenario part of the modified BDD template. Messenger’s daily schedule includes the list of the addresses where is necessary to make a delivery. The messenger picks the closest customer and asks about his availability. When customer approves the delivery, the messenger plans a route to the destination and delivers a package. According to proposed concept the BDD scenario looks as following:

Feature Package delivery – T01

In order to deliver a package.

As messenger (executor)

I want to plan route to destination

Scenario: Planning route to destination

Given I have a list of addresses scheduled for today

When I choose the closest address for the delivery

Then I can find the optimum route to destination via Google Maps

Fig. 8 Example of BDD scenario according to modified template

BDD methodology itself does not strictly recommend how to specify user story for feature description. For the modified approach only one proper definition exists of user story represented by complement transaction composed into BDD scenario. This determines context for the scenarios given in feature description.

BDD scenarios can be validated against production code. They ensure that production code follows activities in company business processes. Also, BDD scenarios are executable and its verification is possible with every upcoming change of information system within continuous integration. The example from Behat framework for the previous BDD scenario is depicted in the Fig. 9.

Feature: Package delivery – T01

In order to deliver a package.

As messenger

I want to plan route to destination

Scenario: Planning route to destination

#features/planning.feature:6

Given I have list of addresses for scheduled for today
#FeatureContext::iHaveListOfAddressesForScheduledForToday()

When I choose the closest address for the delivery
#FeatureContext::iChooseTheClosestAddressForTheDelivery()

Then I can find the optimum route to destination via Google Maps

#FeatureContext::iCanFindTheOptimumRouteToDestinationViaGoogleMaps()

1 scenario (1 passed)

3 steps (3 passed)

0m 0.01s (9.55Mb)

Fig. 9 Output from Behat testing framework after execution of story derived from DEMO transaction

IV. METHOD FOR IDENTIFICATION OF BUSINESS RELEVANT FEATURES

DEMO transactions and BDD scenarios are foundation stones for the proposed method which evaluates relevancy of information systems features. Each step of the method in the list below will be explained in this chapter.

The method includes following tasks:

1. Identification of transactions according to DEMO methodology.
2. Convert identified transactions into the form of BDD scenarios.
3. Map BDD scenarios to current implementation of features.
4. Identify supported and unsupported coordination and production acts by the information system.
5. Identify features of IS to be removed or refactored due to inconsistency to its ontological description.

As an explanatory case is used a brief description of existing company in the Fig. 10.

The company supply of electricity for customers and offers “smart measuring” service which makes them a possibility to monitor the consumption of electricity online. Customers have provided the information system which **reports electricity consumption and savings for each period (T01)**. *Measuring devices broadcast consumption data. This data is stored to database (C01)*.

At the beginning, a client contacts the company and *salesman gives to a potential customer a detailed overview about offered services (C02)*. **When a client signs a contract (T02)**, *contract details are entered into the IS (C03)*. Consequently, *manufacturing of devices is requested (C04)*. The device manufactory department has their own employees and stock of material. Upon the contract, **device arrangements are complemented (T03)**. Once devices are prepared to expedition, *the service department is notified about necessity of installation contracted devices (C05)*. Firstly, installation place is examined by technician who will *decide whether installation is feasible (C06)*. After that, **installations of appliances are planned (T04)**. Planning of appliance installation is a complex process which *considers availability of company cars (C07)*, *booking of accommodation (C08)*, *customer confirmation and skills of technicians (C09)*. *The manager also assigns a specific task to technicians if the customer is available*. **Once the device is installed (T05)**, *a customer signs the montage sheet (C10)*. When the *installation of devices is confirmed (C11)*, a new client is *entered to information system (C12)* and contracted **services starts to be billed (T06)**.

Fig. 10 Text description of company business processes

In the first step of procedure, several transactions have been identified. In the Fig. 10, bold text refers to production facts and blue italic to coordination and production acts. Each transaction consists of coordination and production acts.

- **T01** – Consumption of electricity is reported for each period.
- **T02** – Client signed contract.
- **T03** – Devices arrangements are complemented.
- **T04** – Appliance installation is planned.
- **T05** – Contracted devices are installed.
- **T06** – Services started to be billed.

The second step requires conversion of transactions to BDD scenarios. The case example for the transaction **T04** is depicted in the Fig. 11.

Feature Package delivery – T04

In order to plan the appliance installation

As manager

I want to assign task to the technician

Scenario Outline: Task planning

Given manager has chosen <date>

And car is available on <date>

And technician has no others task on <date>

When customer confirmed availability on <date>

Then task is assigned to technician

Examples:

date	
2017-05-06	
2017-05-07	

Fig. 11 Converted coordination act defined in the transaction **T04** (Gherkin DSL language syntax)

In the third step, converted transactions into BDD scenarios are mapped to production code. This is usually done via frameworks like Cucumber, Behat and the others. Authors recommend to follow instructions for the chosen framework.

```
/**
 * @Given car is available on :date
 */
public function carIsAvailableOn($date)
{
    assertEquals(true,
        $this->carpark->
            hasAvailability($date));
}

/**
 * @Given technician has no others task
 * on :date
 */
public function
technicianHasNoOthersTaskOn($date)
{
    assertEquals(true, $this->
        technician->isAvailable($date));
}

/**
 * @When customer confirmed availability
 * on :date
 */
public function
customerConfirmedAvailability($date)
{
    assertEquals($date,
        $this->order->installDate);
}
```

```
/**
 * @Then task is assigned to technician
 */
public function
taskIsAssignedToTechnician()
{
    assertEquals(true, count(
        $this->technician->tasks) > 0);
}
```

Fig. 12 Example of mapping of modified BDD scenarios to production code (Behat framework implementation)

The fourth step identifies supported (green) and unsupported (red) coordination and production acts by the information system. Unsupported coordination/production act means that it has no reference to any BDD scenarios which have been successfully mapped in the previous step. Result of the fourth step is depicted in the Fig. 13.

The company provides supply of electricity for customers and offers “smart measuring” service which makes it possible for them to monitor their consumption of electricity online. Customers have provided the information system which **reports electricity consumption and savings for each period (T01)**. *Measuring devices broadcast consumption data. This data is stored to database and verified (C01)*.

At the beginning, a client contacts the company and *salesman gives to a potential customer a detailed overview about offered services (C02)*. **When a client signs a contract (T02)**, *contract details are entered into the IS (C03)*. Consequently, *manufacturing of devices is requested (C04)*. The device manufactory department has their own employees and stock of material. Upon the contract, **device arrangements are complemented (T03)**. Once devices are prepared to expedition, *the service department is notified about necessity of installation of the contracted devices (C05)*. Firstly, installation place is examined by technician who will *decide whether installation is feasible (C06)*. After that, **installations of appliances are planned (T04)**. Planning of appliance installation is a complex process which *considers availability of company cars (C07), booking of accommodation (C08), customer confirmation and skills of technicians. Manager also assigns a concrete task to technicians (C09)*. **Once the device is installed (T05)**, *a customer signs the prepared montage sheet (C10)*. When the *installation of devices is confirmed (C11)*, *a new client is entered to information system (C12)* and **contracted services starts to be billed (T06)**.

Fig. 13 Differentiation of supported and unsupported coordination/production acts

Unsupported acts are listed for further investigation of whether such acts could be automated or supported by information systems. Thereby, highly relevant information is

discovered for development of future features to support business processes in the company.

Summary of unsupported coordination/production acts:

- Request for device manufacturing.
- Providing information about offered services to customer.
- Accommodation booking process.
- Notification about appliance installation.
- Making decision whether installation is feasible.
- Checking availability of cars in a company car park.
- Preparation of montage sheet to be signed by a customer.

The fifth step involves the identification of feature specifications (user story, use case, etc.) which are not included in any transaction. In other words, they have no reference to user stories (coordination/production acts) mentioned in mapped BDD scenarios. These features are candidates to be either refactored or removed from the information system. Unfortunately, this should be consulted with product owner, or domain expert. Some functionalities might be foundation elements for the information system, for example user administration. Features which are included in coordination/production acts defined in BDD scenario are linked by identification number from the text description. Feature specifications might differ from project to project. Presented case uses user scenarios technique. The example is depicted below.

- UC 1 Appliance installation evidence.
 - US 1.1 Customers [C12, C09]
 - US 1.2 Reporting from installation [C01]
- UC 2 Device management
 - US 2.1 Data broadcast testing [C01]
 - US 2.2 Remote reset [ref is missing]
- UC 3 Planning of appliance installations
 - US 3.1 Task planning [C03]
 - US 3.1.1 Customer confirmation [ref is missing]
 - US 3.1.2 Technician skill evidence [ref is missing]
 - US 3.2 Technician utilization overview [C09]
- UC 4 Announcements
 - US 4.1 News board [ref is missing].
 - US 4.2 Personal messages [ref is missing]

Fig. 14 Identification of business irrelevant features

V. DISCUSSION AND FUTURE RESEARCH

Ontological nature of transactions presumes an existence of essential business processes. Hence, the proposed method is suitable especially for development of software products which supports business processes in companies. Once the transactions became a part of BDD scenarios, it involves the developer or analyst to understand purpose why the feature is implemented. Also, it sets boundaries for the BDD

scenarios which are consequently linked to the existing essence of the business.

The most important benefits of proposed approach:

1. Text descriptions for derivation of transactions are humanly-readable, hence there is no problem to have descriptions validated by employees in company.
2. The method detects instantly which coordination and production acts are supported by information system.
3. Also, it finds useless feature which is possible to remove or not maintain anymore.
4. Production code base, respectively features are linked to ontological description of business processes.
5. Instant feedback through automated testing.

Contrary, the method does not work well with the development of software which is not going to support business processes. Another problem is the fact that companies evolve over time and change their business processes. Therefore, text descriptions need to be updated as development goes on. Consequently, it is necessary to propagate modifications into scenarios and information system to avoid technical debts. Unfortunately, this will always stay up to responsibility of the company and software developers.

The identification of feature relevance is one of the most challenging part in the refactoring process, especially for applications with huge technical debt, which desire radical refactoring where is hardly possible to save all existing features in order to settle technical debt quickly. In addition, relevancy of features for business intentions is critical in terms of further investments for already existing information systems. Authors also work as software developers and due to their experience, irrelevant features are not something that rarely occur in the implementation of any information system.

The presented method also discovered another important finding. The action model defined in DEMO methodology represents internal business rules for coordination and production acts. Such business rules should be reflected in the information systems. The example of action model definitions is depicted below.

on stated T02(M,Y)

```

if <installation is feasible> ≥ accept T02(M,Y)
¶not <installation is feasible> ≥ reject T02(M,Y)
fi

```

```

if <some other condition> ≥ reject T02(M,Y)
¶not <some other condition> ≥ state T03(M)
fi

```

no

Fig. 15 Action model example

These definitions are also executable. Nevertheless, the question remains whether it is also possible to include them into BDD scenarios and verify during software testing. This will be an objective of further research.

VI. CONCLUSION

The main contribution of the paper resides in presentation of method which interconnects ontological models of business processes directly to information system features implementation and allows to evaluate their relevancy for enterprise, whereby it provides a clear differentiation of features which are or not important for performing tasks by employees in enterprise. This method could help to reduce the technical debt of current information systems and identify main endpoints and interfaces that are candidates for refactoring.

ACKNOWLEDGMENT

The paper was supported by the grant provided by Ministry of Education, Youth and Sport Czech Republic, reference no. SGS15/PRF/2017.

REFERENCES

- [1] M. Cohn, *User stories applied: for agile software development*. Boston: Addison-Wesley, 2004, pp. 31–41.
- [2] J. F. Smart, *BDD in action: Behavior-Driven development for the whole software lifecycle*. New York: Manning Publications Company, 2014, pp. 3–32.
- [3] J. L. G. Dietz, *Enterprise ontology: theory and methodology*. New York: Springer, 2006, pp. 16–31.
- [4] J. Zacek, J. Matula, and F. Hunka, Context definition for BDD scenarios upon DEMO methodology, 2nd International Conference on Theory and Practice, Sia Pacific Institute of Advanced Research, 2016, pp. 164–169, ISBN 9780994365613.
- [5] J. Matula, J. Zacek, and F. Hunka, Relevant User Stories by Using DEMO Analysis, Proceedings of the 11th Scientific Conference Internet in the Information Society, University of Dabrowa Górnicza, Cieplaka, 2016. pp. 21–30. ISBN 9788365621009.
- [6] S. J. H. Van Kervel, *Ontology driven enterprise information systems engineering*, 2012.
- [7] M. Pesic and W. M. Van der Aalst, A declarative approach for flexible business processes management, *Business Process Management Workshops*, Springer Berlin Heidelberg, 2006, pp. 169–180.
- [8] B. N. Groszof, Y. Labrou, and H. Y. Chan, A declarative approach to business rules in contracts: courteous logic programs in XML, *Proceedings of the 1st ACM conference on Electronic commerce*, 1999, pp. 68–77.
- [9] M. de Leoni, F. M. Maggi, and W. M. van der Aalst, An alignment-based framework to check the conformance of declarative process models and to pre-process event-log data, *Information Systems*, 2015, pp. 258–277.
- [10] M. G. Skjæveland, M. Giese, D. Hovland, E. H. Lian, and A. Waaler, Engineering ontology-based access to real-world data sources, *Web Semantics: Science, Services and Agents on the World Wide Web*, 2015, pp. 112–140.
- [11] G. Gigante, F. Gargiulo, and M. Ficco, A semantic driven approach for requirements verification, *Intelligent Distributed Computing VIII*, 2015, pp. 427–436.

Temporal Evaluation of Business Processes Using Timed Colored Petri Nets

Yoshiyuki Shinkawa

Graduate School of Science and Technology
Ryukoku University

1-5 Seta Oe-cho Yokotani, Otsu, Shiga, Japan
Email : shinkawa@rins.ryukoku.ac.jp

Ryoya Shiraki

Graduate School of Science and Technology
Ryukoku University

1-5 Seta Oe-cho Yokotani, Otsu, Shiga, Japan
Email : t16m081@mail.ryukoku.ac.jp

Abstract—Time constraints become one of the most crucial requirements to be satisfied in business processes, in order to make the business competitive, and to achieve the business goal. This paper proposes a Colored Petri Net (CPN) based approach to modeling and evaluating business processes including various temporal constraints and requirements. The essential part of a business process and temporal aspects are separated in our approach to make the business process models comprehensive. More specifically, separately-defined modules to deal with time constraints are to be appended to the traditional non-temporal business process models. The created models can be simulated using “cpntools” to evaluate whether the given temporal requirements are satisfied.

I. INTRODUCTION

THE evolution of information and communication technologies, along with the growth of the Internet, makes time constraints in business more important than what they were in the pre-Internet ages. This evolution also makes business processes [1] more complicated, since there are many alternatives available regarding information storage and retrieval, process automation, exception handling, and so on. In these circumstances, we need to include various information into business process models, such as data processing options, current and future availability for related resources, complicated decision rules to optimize the business, business and legal rules that regulate the process, and time constraints with statistical and probabilistic properties [2].

However, traditional business process modeling and specification languages like BPMN (Business Process Modeling Notation) [3] and BPEL (Business Process Execution Language) [4] mainly focus on task flows and their relationships within a business process. Even though several trials have been made to extend these languages from the temporal viewpoint, they do not provide us with enough capability to express the above information yet [5][6]. In order to express today’s complicated business processes, we need a modeling tool which can reflect the following aspects of a business process.

- 1) Requirements and availability of material, human and financial resources
- 2) Business and legal rules regulating each task or the whole process
- 3) Task and process related data, along with their transformation rules

- 4) Temporal requirements to the process, such as response time and throughput
- 5) Temporal properties of each task and resource, such as mean execution time and mean resource retention time along with the variance.

Consequently, a modeling tool for business processes must provide us with the capability to depict the four aspects of a business process, namely, the structural, functional, behavioral, and temporal aspects. In addition, logical and probabilistic properties must be precisely expressed in the business process models.

Colored Petri Net (CPN) [7] is one of the comprehensive modeling tools satisfying the above requirements, since it can depict the structure of a system as a directed bipartite graph, the complicated regulation and transformation rules that reside in a system as functions written by CPN ML language, the data structure as color sets, the temporal requirements and facts as timed color sets, and probabilistic and statistical properties using the library functions provided as a part of CPN ML language.

This paper proposes a CPN based approach to modeling and evaluating time constraints in business processes. The paper is organized as follows. In section 2, we discuss various time constraints that reside in business processes, in conjunction with their probabilistic and statistical properties. Section 3 introduces Colored Petri Net (CPN) along with its temporal expression capability. Section 4 presents how complicated business processes including time constraints are modeled using CPN. Section 5 shows an evaluation of time constraints in business processes expressed in the form of CPN.

II. TIME CONSTRAINTS IN BUSINESS PROCESSES

In this section, we introduce possible time constraints that reside in business processes. Before discussing it, we first define the basic business process structure briefly.

A. The Essential Structure of a Business Process

There could be many viewpoints to a business process depending on the purpose of business process modeling, which include behavioral, functional, structural, financial, and temporal ones. In addition each business process modeling tool provides us with its unique model elements from its own

perspective to business. Therefore we need to build multiple business process models using multiple modeling tools reflecting the above multiple viewpoints. However, in order to define time constraints in a business process rigorously, it is desirable to build a unified model which reflects all the essential elements among those multiple models.

Generally speaking, the simplest form of a business process is a set of task flows, where a task represents an indecomposable unit of work that configures the business process. Upon this simplest model, the following information should be added to make its semantics clear.

- 1) The organizations and human resources that engage in the business process
- 2) The materials to be dealt with by the business process
- 3) The financial resources which are required to execute the business process
- 4) The business and legal rules to regulate the business process
- 5) The goals and strategies behind the business process

The representation and notation of the above information are shown in section 4.

B. Time Constraints in Business Processes

There are two contrastive aspects of time constraints in business processes. One is the time-related requirements to a business process or a task, which must be satisfied by the implemented business process. The other is the time-related properties of each task or resource, which restrict the behavior of them. The former are given in the form of *points in time* or *durations*. For example, the requirements such as “the task must start at 9:00AM” and “the whole process must end by 6:00PM” designate specific points in time, and are often referred to as *deadlines*, while “the task must end within one hour” and “the whole process must end within three days” designate durations.

On the other hand, the latter are not usually given as specific values, instead we have to monitor and measure each task and resource in order to obtain the values. Unlike the physical events, business events are unstable and therefore most of the measured values are statistical. As a result, each value is given as a set of a mean value and variance with an appropriate distribution function. For example, the value is given in the form of “the mean execution time of the task is 5 minutes, the variance is 4, and follows the normal distribution”, or “the mean term of validity for the resource is 5 days, the variance is 2, and follows the gamma distribution”. In some cases, these values are given as fixed values without measurement, which include the values given by material specifications, business rules like employment regulation, or legal rules. For example, the expiration date of a material, the retirement date of an employee, and the warranty period of a product are the temporal properties given as fixed values.

The above temporal properties usually cause the delays in a business process, mainly at task initiation or during task execution. The delay mechanism is not so simple since there are several factors to cause the delays, and we have to take

the combination of them into account. The first factor is the task execution time that can fluctuate following a distribution function that is associated with the task. The second is the resource waiting time, during which the related tasks are halted until the resources become available. These resources could be material, human, or financial ones. The third is the service waiting time, during which some serving mechanism is busy even though all the related resources are available. In this situation, tasks are waiting in a queue in terms of the *queuing theory* [8]. The last is the rule based waiting time, during which the tasks are halted because of some business or legal rules. This case includes financial audit, facility inspection, and complaint handling which might stop the task execution.

As discussed above, time constraints in a business process are so complicated that we cannot handle them using traditional task flow based business process models. We need more information-rich models which reflect not only the behavioral aspect of a business process, but also the functional, data, and temporal aspects along with various kinds of rules that regulate the business process. In this paper, we use Colored Petri Net (CPN) for this purpose. In the next section, we give a brief description of this technique.

III. COLORED PETRI NET AND TIME CONSTRAINTS

The original Petri net, often referred to as a regular Petri net or a place-transition (PT) net, is a directed bipartite graph with two kinds of nodes called “*transition*” and “*place*”, which are alternately connected by directed arcs [9]. In a model written by CPN, or a CPN model for short, a transition represents an event which could occur in a system, while its preceding places represent the pre-conditions for its occurrence, and its succeeding places represent its post-conditions. Each preceding place can be marked by *tokens* to represent the corresponding condition holds. If all the preceding places are marked by tokens, the transition becomes eligible to fire. The transition firing represents an occurrence of the event, and the tokens in the preceding places are transferred to the succeeding places.

Even though the regular Petri net can express the behavior of distributed concurrent systems rigorously, there are several aspects of a system difficult to be represented by it, such as functional (or data transformational), temporal, probabilistic, statistical, and logical aspects. In order to relieve these difficulties, there have been many extensions to it proposed. Colored Petri net (CPN) is one of these extensions which makes it possible to

- 1) assign a data type to each token which is referred to as a *color*
- 2) set the values to a token according to the color definition
- 3) assign a function to an arc to manipulate the values that are set to tokens
- 4) assign a function to a transition to control its firing, which is referred to as a *guard*
- 5) define variables for representing the tokens moving within a CPN model

CPN is formally defined as a nine-tuple $CPN=(P, T, A, \Sigma, V, C, G, E, I)$, where

P : a finite set of places.
 T : a finite set of transitions.
 (a transition represents an event)
 A : a finite set of arcs $P \cap T = P \cap A = T \cap A = \emptyset$.
 Σ : a finite set of non-empty color sets.
 (a color represents a data type)
 V : a finite set of typed variables.
 C : a color function $P \rightarrow \Sigma$.
 G : a guard function $T \rightarrow \text{expression}$.
 (a guard controls the execution of a transition)
 E : an arc expression function $A \rightarrow \text{expression}$.
 I : an initialization function : $P \rightarrow \text{closed expression}$.

While the CPN is an extension of the original Petri net to express the functionality of a system, there is another extension to express the temporal properties. This extension is referred to as “timed Petri nets” [10]. The CPN can be extended to the *timed* CPN by appending a *timed* property to each token through the color definition. This property gives a *clock timer* to a token, which can postpone the transaction firing until the timer expires. The clock values can be set or reset by arc functions or transaction firing. This simple mechanism makes it possible to express, analyze, and evaluate complicated systems including various temporal events. In the next section, we discuss how the business processes with time constraints are modeled using timed CPN.

IV. MODELING A BUSINESS PROCESS BY CPN

As discussed in section 2, business processes and time constraints are complicatedly interrelated and therefore the business process models including time constraints also become complicated. In order to relieve this model complexity, we build a model by combining three independent CPN models or modules, namely, the base module to represent the essential part of the business process without the time constraints, the delay module to represent the task and resource delays, and the queue module to represent the service waiting time in terms of the queuing theory.

A. The Base Module

This module represents a business process without time constraints, which shows its non-temporal logical aspects. There have been several researches to apply CPN to business processes [11][12][13]. Since the most essential part of a business process is a set of task flows, we focus on a task as a basic element to be modeled by CPN. As discussed previously, a task is an atomic unit of work in a business process, and four kinds of resources are required to perform it, namely, human, material, financial, and information (or data) ones. In CPN model, these resources are represented as *tokens*, and the kinds of tokens are distinguished by *colors*. Each color must include the following information as properties.

[Human Resource Color]

This color represents a person or personnel involved in the business process. The basic information that the color should

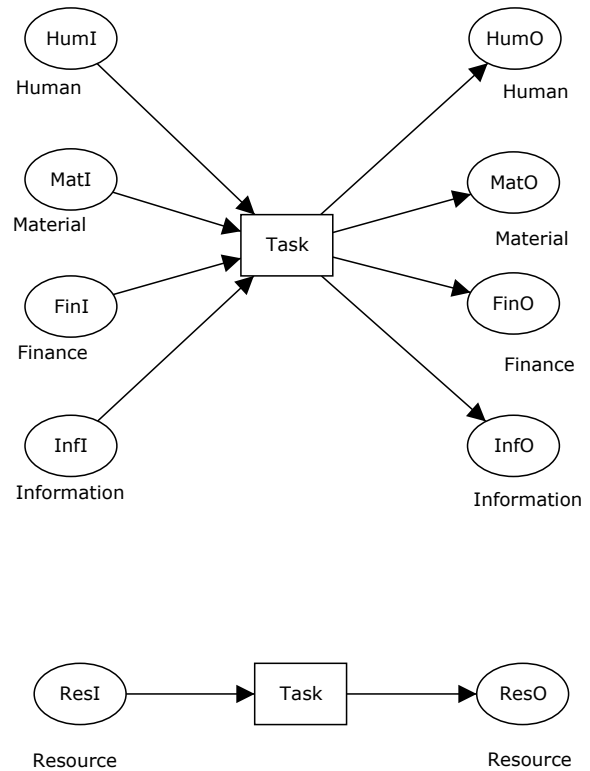


Fig. 1. Basic Task Unit

include is the sort of occupation, own department, post and rank, and salary level.

[Material Resource Color]

This color represents a material to be dealt with by each task. The properties that the color should include are the type of the material, price, quantity, and supplier.

[Financial Resource Color]

This resource represents the required operating capital to perform a task. The properties that the color should includes are the purpose, funding source, amount, and responsible department.

[Information Resource Color]

This color represents the information that is needed to perform a task. The information is provided mainly in the form of data, however in some cases, provided by documents, phones, or faxes. The color should include the type of contents, media of the information, source of the information, and the type of operations to be applied.

As the first step, we define each of the above properties as an integer type color, and the meaning of each value that a color takes is interpreted in CPN ML functions to be defined for arc and guard functions. These values could be unique for each business process. For example, the color set definition for the human resource in some business process is

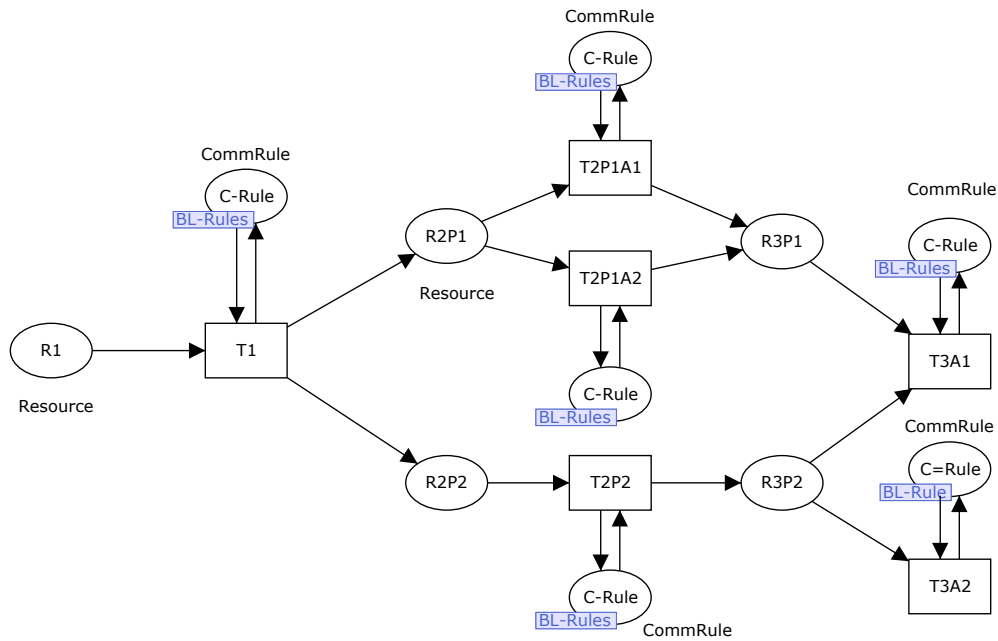


Fig. 2. Business Process Base Module

closet Human = product Occup * Dep * Pos * Rank * Salary;

where each element of the direct product is defined as “INT” type, and the meaning of each value is interpreted in the model, e.g. the value “1” of the color “Occup” means an *engineer*, value “2” means a *sales representative*, and so on.

Since each task manipulates the above four types of color sets, and transforms them as new tokens to be passed to the succeeding tasks, its structure in a CPN model is depicted as shown in the upper figure of Fig. 1. Even though it seems natural to assign the above “resource” colors to the tokens, it could increase the number of tokens, and make the guard and arc function complicated. In order to reduce the number of tokens, and make the functions simple, we use the list of tokens like

closet HumanList = list Human;

In addition, we can reduce the number of task input places by defining the tuple of these lists like

closet Resouce = product HumanList * MaterialList * FinancialList * InformationList;

This closet makes it possible to integrate the four input and output places into a pair of single places as shown in the lower figure of Fig. 1, and this CPN structure is to be used as a basic task unit in this paper. Once the basic unit of business process models is defined, the next step is to combine them into a whole process model that represents all the possible task flows. In order to make this model executable, we have to define guard functions and arc functions appropriately

so that they reflect the business, legal and other kinds of rules regulating the business process. These rules are divided into two categories, namely, task unique (or local) rules and business process wide (or global) rules. Each task unique rule controls the transition firing using the information in the input token, and determines the information to be passed to the succeeding tasks through the output tokens. On the other hand, each business process wide rule affects possibly all the task executions using global common rules. These common rules, which include business and legal rules along with social and commercial practices, are represented in the form of CPN ML list, each element of which corresponds to a rule expressed as an integer list. Each guard or arc function is to be responsible for the interpretation and implementation of this integer list. As a result, only one token with the color defined as a list of integer list represents all the global rules, and consequently only one place is used to hold the global rules. This implementation makes the CPN structure simple, since only one arc is needed to access the global rules. Fig. 2 shows a simple implementation of a business process base module expressed in the form of CPN. We use the following naming convention to make the models readable.

- 1) A transition representing a task is labeled “ $T_iP_jA_k$ ”, where “ T_i ” represents the i -th task, “ P_j ” represents the task is to be performed in parallel as the j -th occurrence, and A_k represents the k -th alternative in a selective task execution.
- 2) A place representing a resource is labeled “ R_iP_j ”, which represents the resource is used for the task “ $T_iP_jA_k$ ”. Since only one place is needed for aselective task execution, no “ A_k ” is used.

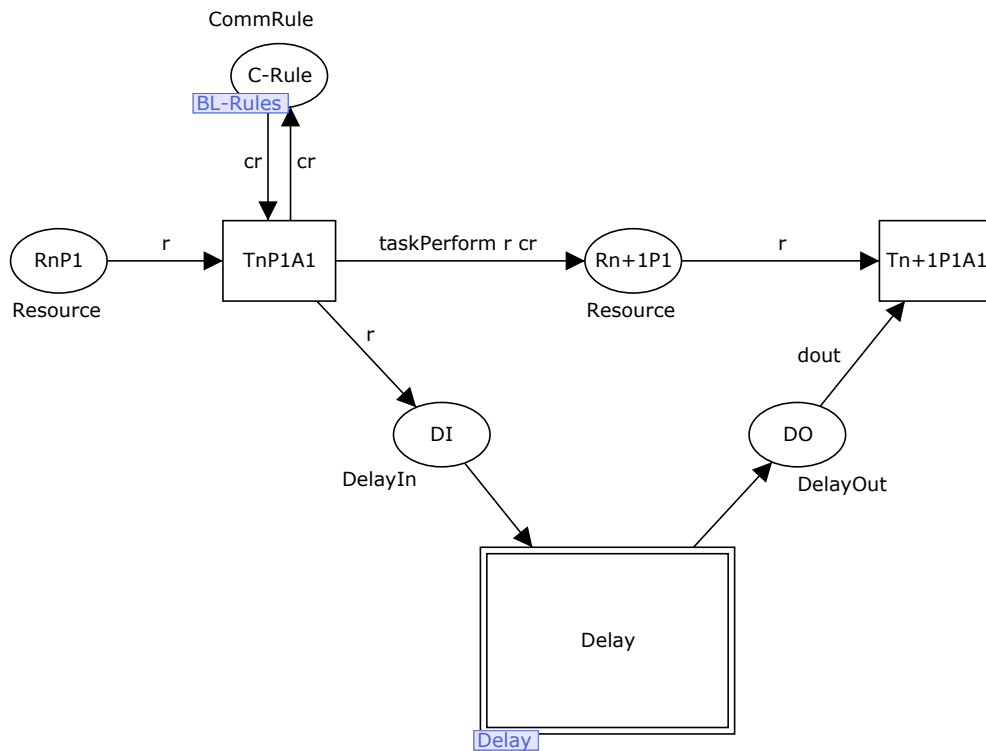


Fig. 3. Independent Delay Module

3) The place for the common rules is labeled “C – Rule” with the *fusion* tag “BL – Rule”. A *fusion* place in CPN model represents that the different places in a model designate the same place.

By using the above fusion place, we can avoid to use long arcs to access the common rules.

B. Delay Module

The purpose of this module is to implement temporal delays caused by task execution, resource waiting, or business or legal rules. A natural implementation of the delays in a CPN model is to increment a timestamp of each related token at a transition firing or by an arc function to postpone the next transition firing. However, this approach makes the CPN model complicated, since the temporal information spreads over the model. In addition, this information divergence makes the model maintainability worse. In order to avoid this difficulty, we concentrate the temporal information in an independent module connected to the transitions that the delays are expected. Fig. 3 briefly shows this approach. In this figure, the independent module “Delay” is inserted between the task transition “ $T_nP_1A_1$ ” and “ $T_{n+1}P_1A_1$ ” through the two places “DI” and “DO”. This module with these places can be inserted between any two consecutive task transitions, and it prevents the divergence of the delay mechanism over the model. Fig. 3 shows the interrelation between the base module and delay module, and composed in the following way.

- 1) Prepare two additional places “DI” and “DO” to the original CPN model, where “DI” is used as the input to the delay module, while “DO” is the output place from it.
- 2) Draw an arc from the transition that delays are expected to “DI”. This transition is referred to as “deferred transition”.
- 3) Assign a variable (the variable “ r ” in Fig. 3) representing the resource for the delay transition to this arc.
- 4) Draw an arc from the delay module to the above new output place “DO”. The color associated with this new place is an integer with a timestamp. A token with this color is referred to as “delayed token”, and the integer value represents the id of a task.
- 5) Draw an arc from this new output place to the succeeding transitions from the delayed transition.

The firing of the succeeding transition, which represents the next task execution, is postponed arbitrarily by setting the timestamp of the “delayed token”. Since the delay of each task transition is determined by the resource status and the global rules, one of the simplest implementations of the “delay module” is as shown in Fig. 4. In this figure, the transition “Analyze” is responsible to examine the resource status to compose the parameter to be passed to the delay calculation function “genDelay”. On the other hand, the transition “DCalc” determine the actual delay time using the above parameter and the global rules.

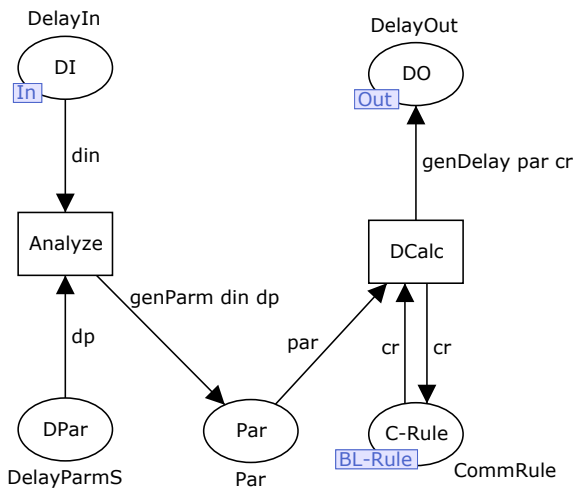


Fig. 4. An Implementation of Delay Module

C. Queue Module

In addition to the above explicitly defined delays, there is a different type of delays called a “wait”. The concept of the wait is introduced in the queuing theory [8], which represents the delay caused by server unavailability. In business processes, this server corresponds to one of the person, organization, or facility, which is responsible for a task. In order to make the model simple, we build an independent module that realizes this type of delay, in the similar way we did for the delay module. This module is shown in Fig. 5, and composed as follows.

- 1) Add the “Queue” module with two additional places “Count” and “Arrival” to the original CPN model including the “Delay” module.
- 2) Draw a bi-directional arc between the input place “DI” and the queue module.
- 3) Draw a bi-directional arc between the “Count” place and the queue module, and between the “Count” place and the succeeding transition $T_{n+1}P_1A_1$ in Fig. 5.
- 4) Draw a uni-directional arc from the queue module to the “Arrival” place.
- 5) Draw an uni-directional arc from the “Arrival” place to the delay module.

The queue module works as follows.

- 1) The place “Count” holds an integer token representing the number of concurrently available servers.
- 2) When the task “ $T_nP_1A_1$ ” ends, a token is passed to the place “DI” to determine the delay.
- 3) The guard of the queue module makes the module fireable if the token value in the “Count” place is positive. This guard examines the server availability.
- 4) The above firing passes a token to the “Arrival” place to make the delay module fireable.

The above mechanism implements the queuing model for a single task execution, and is to be deployed over the CPN model where the temporal delays are expected. The internal

structure of the queue module is quite simple as shown in Fig. 6.

V. EVALUATION OF TIME CONSTRAINTS

The CPN models discussed in the previous section reflect temporal properties and constraints associated with the resources and tasks that occur in the business processes. In order to evaluate the business processes from temporal viewpoints, we need to execute the models using the cpntools [14]. For this simulation, the following data are required and must be set in appropriate tokens.

- 1) Initial resource status for the business process to be simulated, including human, material, and financial resources. These data are set in the resource list tokens which are marked in the input place of each task transition.
- 2) Business and legal rules that are to be applied to the business process. These data are set in the rule list token which is marked in the global rule place.
- 3) The number of concurrent executions for each task. These data are set in the tokens which are marked in the “Count” place.

After the simulation, we have to examine the timestamp of each timed token to determine whether the given temporal requirements are satisfied. For this purpose, we need to distinguish each business process instance in the simulation result. However, each token in our CPN model does not have enough information to identify to which business instance it belongs. Therefore, we add a sequence number to all the task-related tokens, which represents the process instance identification. This mechanism is implemented by modifying the CPN models as shown in Fig. 7 and is composed in the following way¹.

- 1) Add a place (the “PISeq” place in Fig. 7) to control the sequence number, which is marked by a timed INT type token initialized as 1.
- 2) Each business process initiation task transition, that is, a task transition having no preceding task, obtains the above token to get the sequence number of the process instance to be initiated, and pass it back incrementing the value by 1.
- 3) Add a new place “Trace” to hold the temporal events such as task execution, initiation, or termination in the form of a list. This list is referred to as a *trace list*.
- 4) Each process initiation task transition appends the above token including the sequence number to the trace list.
- 5) Each time a task transition other than the above ones fires, it appends a token in “DO” place to the trace list.
- 6) After a simulation ends, the *trace list* includes task execution history with timestamps.

By analyzing the above trace list, we can evaluate whether the temporal requirements are satisfied. This analysis can be

¹In Fig. 7, the “Delay” module and “Queue” module are integrated into a single module “Delay and Queue” in order to make the figure concise.

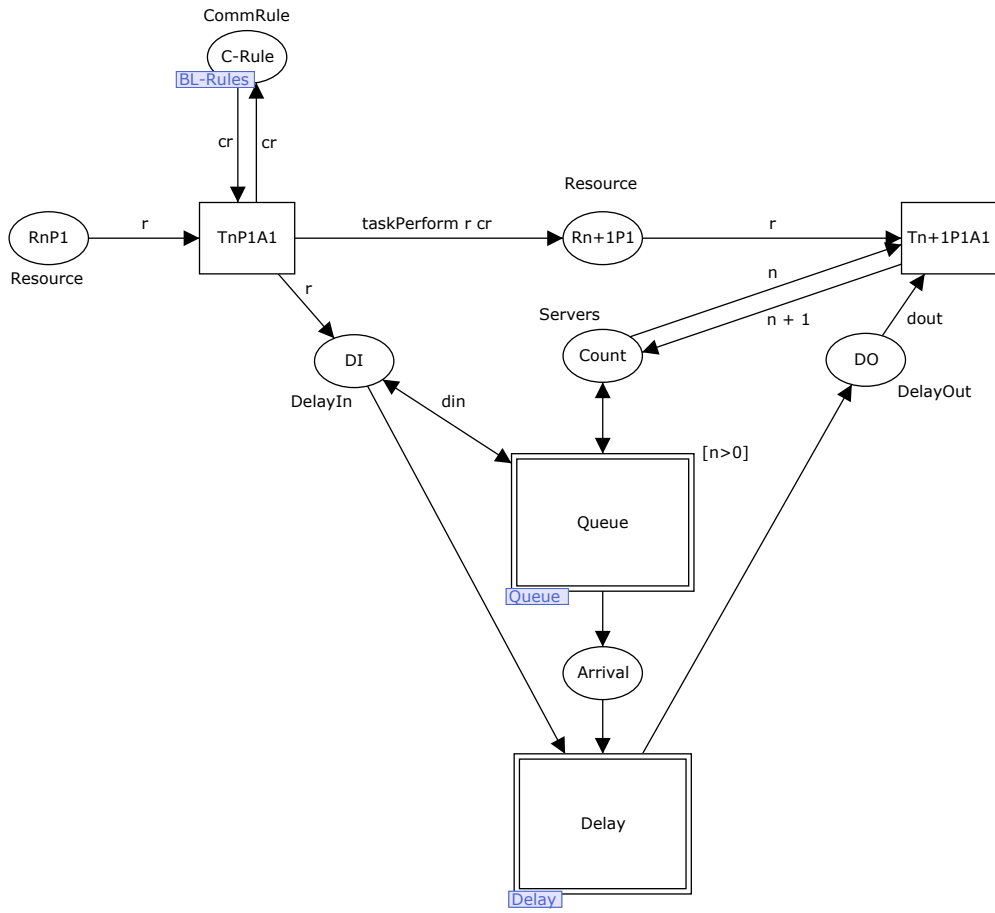


Fig. 5. Independent Queue Module

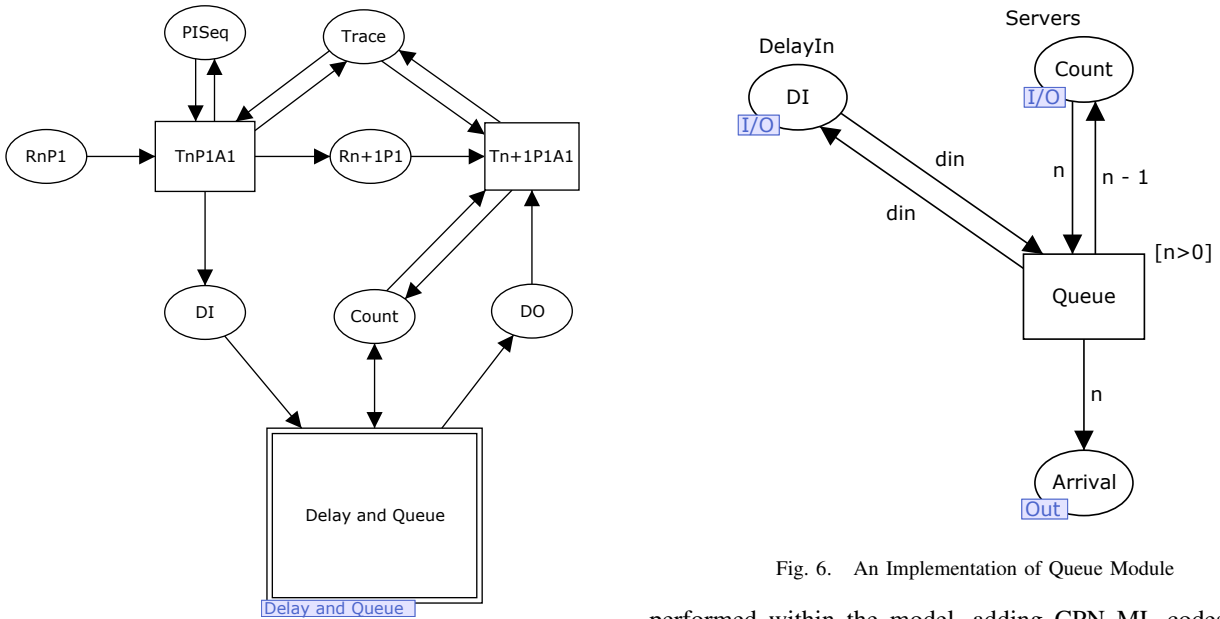


Fig. 6. An Implementation of Queue Module

Fig. 7. Evaluation of Time Constraints

performed within the model, adding CPN ML codes to the model.

VI. CONCLUSIONS

Business processes become more and more complicated for various reasons, e.g. intensified competition, deregulations, new regulations, business and technology innovation, and business globalization. These factors require business process models to deal with temporal properties more precisely. However traditional business process modeling tools are furnished with few capabilities to deal with them.

In this paper, we propose a Color Petri net (CPN) based approach to modeling and evaluating the business processes from temporal viewpoints. We first model the business processes without time constraints, including various business and legal regulations along with resource based constraints. Succeedingly, we added the temporal modules to them with minimal modification of the original models. Finally, we added the evaluation mechanism to the modified models. Our approach needs many CPN ML codes and functions, and currently they must be built for each individual model, which lowers the evaluation efficiency. The next step of this research is to manage and reuse these codes and functions.

REFERENCES

- [1] M. Dumas, M. La Rosa and J. Mendling, *Fundamentals of Business Process Management*, Springer, Heidelberg, Germany; 2013.
- [2] S. Cheikhrouhou, S. Kallel, N. Guermouche, and M. Jmaiel, "The temporal perspective in business process modeling: a survey and research challenges," *Service Oriented Computing and Applications* vol. 9, issue. 1, 2015, pp. 75–85. [Online]. Available: <http://dx.doi.org/10.1007/s11761-014-0170-x>
- [3] B. Silver, *BPMN Method and Style, 2nd Edition, with BPMN Implementer's Guide: A Structured Approach for Business Process Modeling and Implementation Using BPMN 2*, Cody-Cassidy Press, Altadena, CA; 2011.
- [4] M. B. Juric and D. Weerasiri, *WS-BPEL 2.0 Beginner's Guide*, Packt Publishing, Birmingham, UK; 2014.
- [5] D. Gagne and A. Trudel, "Time-BPMN," *Proc. of 2009 IEEE Conference on Commerce and Enterprise Computing*, pp. 361–367, 2009. [Online]. Available: <http://dx.doi.org/10.1109/CEC.2009.71>
- [6] H. Banati, P. Bedi and P. Marwaha, "Extending BPEL for WSDL-Temporal based Web services," *Proc. of 12th International Conference on Hybrid Intelligent Systems (HIS)*, pp. 484–489, 2012. [Online]. Available: <http://dx.doi.org/10.1109/HIS.2012.6421382>
- [7] K. Jensen and L. Kristensen, *Coloured Petri Nets: Modelling and Validation of Concurrent Systems*, Springer, Heidelberg, Germany; 2009.
- [8] V. V. Kalashnikov, *Mathematical Methods in Queuing Theory (Mathematics and Its Applications)*, Springer, Heidelberg, Germany; 2010.
- [9] M. Diaz, *Petri Nets: Fundamental Models, Verification and Applications*, Wiley-ISTE, Hoboken, NJ; 2009.
- [10] J. Wang, *Timed Petri Nets: Theory and Application (The International Series on Discrete Event Dynamic Systems)*, Springer, Heidelberg, Germany; 1998.
- [11] M. Werner, "Colored Petri Nets for Integrating the Data Perspective in Process Audits," *Lecture Notes in Computer Science* vol. 8217, 2013, pp. 387–394. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-41924-9_31
- [12] K. van Hee, O. Oanea, and N. Sidorova, "Colored Petri Nets to Verify Extended Event-Driven Process Chains," in *the 2005 Confederated International Conference on On the Move to Meaningful Internet Systems*, Agia Napa, Cyprus, 2005, pp. 183–201. [Online]. Available: http://dx.doi.org/10.1007/11575771_14
- [13] W. P. M. Aalst and C. Stahl, *Modeling Business Processes: A Petri Net-Oriented Approach*, The MIT Press, Heidelberg, Cambridge, MA; 2011.
- [14] K.Jensen, L. Kristensen, and L. Wells "Coloured Petri Nets and CPN Tools for Modelling and Validation of Concurrent Systems," *International Journal on Software Tools for Technology Transfer (STTT)*, Vol. 9, Numbers 3–4, 2007, pp. 213–254. [Online]. Available: <http://dx.doi.org/10.1007/s10009-007-0038-x>

23rd Conference on Knowledge Acquisition and Management

KNOWLEDGE management is a large multidisciplinary field having its roots in Management and Artificial Intelligence. Activity of an extended organization should be supported by an organized and optimized flow of knowledge to effectively help all participants in their work.

We have the pleasure to invite you to contribute to and to participate in the conference "Knowledge Acquisition and Management". The predecessor of the KAM conference has been organized for the first time in 1992, as a venue for scientists and practitioners to address different aspects of usage of advanced information technologies in management, with focus on intelligent techniques and knowledge management. In 2003 the conference changed somewhat its focus and was organized for the first under its current name. Furthermore, the KAM conference became an international event, with participants from around the world. In 2012 we've joined to Federated Conference on Computer Science and Systems becoming one of the oldest event.

The aim of this event is to create possibility of presenting and discussing approaches, techniques and tools in the knowledge acquisition and other knowledge management areas with focus on contribution of artificial intelligence for improvement of human-machine intelligence and face the challenges of this century. We expect that the conference&workshop will enable exchange of information and experiences, and delve into current trends of methodological, technological and implementation aspects of knowledge management processes.

TOPICS

- Knowledge discovery from databases and data warehouses
- Methods and tools for knowledge acquisition
- New emerging technologies for management
- Organizing the knowledge centers and knowledge distribution
- Knowledge creation and validation
- Knowledge dynamics and machine learning
- Distance learning and knowledge sharing
- Knowledge representation models
- Management of enterprise knowledge versus personal knowledge
- Knowledge managers and workers
- Knowledge coaching and diffusion
- Knowledge engineering and software engineering
- Managerial knowledge evolution with focus on managing of best practice and cooperative activities
- Knowledge grid and social networks

- Knowledge management for design, innovation and eco-innovation process
- Business Intelligence environment for supporting knowledge management
- Knowledge management in virtual advisors and training
- Management of the innovation and eco-innovation process
- Human-machine interfaces and knowledge visualization

SECTION EDITORS

- **Hauke, Krzysztof**, Wroclaw University of Economics, Poland
- **Nycz, Malgorzata**, Wroclaw University of Economics, Poland
- **Owoc, Mieczyslaw**, Wroclaw University of Economics, Poland
- **Pondel, Maciej**, Wroclaw University of Economics, Poland

REVIEWERS

- **Abramowicz, Witold**, Poznan University of Economics, Poland
- **Andres, Frederic**, National Institute of Informatics, Tokyo, Japan
- **Badica, Amelia**, University of Craiova, Romania
- **Berio, Giuseppe**, Universite de Bretagne Sud, France
- **Bodyanskiy, Yevgeniy**, Kharkiv National University of Radio Electronics, Ukraine
- **Chmielarz, Witold**, Warsaw University, Poland
- **Christozov, Dimitar**, American University in Bulgaria, Bulgaria
- **Christozov, Dimitar**, American University in Bulgaria, Bulgaria
- **Grabowski, Mariusz**, Krakow University of Economics, Poland
- **Helfert, Markus**, Dublin City University, Ireland
- **Hussain, Fehmida**, School of Science and Technology, Dubai
- **Jan, Vanthienen**, Katholike Universiteit Leuven, Belgium
- **Jelonek, Dorota**, Faculty of Management of Czestochowa University of Technology
- **Kania, Krzysztof**, Ue Katowice
- **Kayakutlu, Gulgun**, Istanbul Technical University, Turkey
- **Khachidze, Manana**, Tbilisi State University, Georgia
- **Kisielnicki, Jerzy**, University of Warsaw, Poland

- **Konikowska, Beata**, Institute of Computer Science, Poland
- **Korwin-Pawlowski, Michael L.**, Universite du Quebec en Outaouais, Canada
- **Kulczycki, Piotr**, Systems Research Institute, Polish Academy of Sciences, Poland
- **Ligeza, Antoni**, AGH University of Science and Technology, Poland
- **Mach-Król, Maria**, University of Economics in Katowice, Poland
- **Mercier-Laurent, Eunika**, University Jean Moulin Lyon3, France
- **Michalik, Krzysztof**, University of Economics in Katowice, Poland
- **Milewski, Robert**, Medical University of Bialystok, Department of Statistics and Medical Informatics, Poland
- **Nalepa, Grzegorz J.**, AGH University of Science and Technology, Poland
- **Olszak, Celina M.**, University of Economics in Katowice, Poland
- **Opila, Janusz**, AGH University of Science and Technology, Poland
- **Paliński, Andrzej**, AGH University of Science and Technology, Poland
- **Petryshyn, Lubomyr**, AGH University of Science and Technology, Poland
- **Pelech-Pilichowski, Tomasz**, AGH University of Science and Technology, Poland
- **Prasad, T. V.**, Godavari Institute of Engineering and Technology, India
- **Pulvermueller, Elke**, University Osnabrueck, Germany
- **Reimer, Ulrich**, University of Applied Sciences St. Gallen, Switzerland
- **Rossi, Gustavo**, National University of La Plata, Argentina
- **Salem, Abdel-Badeeh M.**, Ain Shams University, Egypt
- **Sankowski, Dominik**, University of Technology in Łódź, Poland
- **Sauer, Jurgen**, University of Oldenburg, Germany
- **Schroeder, Marcin Jan**, Akita International University, Japan
- **Skalna, Iwona**, AGH University of Science and Technology, Faculty of Management, Poland
- **Sobińska, Małgorzata**, Wrocław University of Economics, Poland
- **Soja, Piotr**, Cracow University of Economics, Poland
- **Stawowy, Adam**, AGH University of Science and Technology, Faculty of Management, Poland
- **Surma, Jerzy**, Warsaw School of Economics, Poland and University of Massachusetts Lowell, United States
- **Szpyrka, Marcin**, AGH University of Science and Technology, Poland
- **Teufel, Stephanie**, University of Fribourg, Switzerland
- **Tvrdikova, Milena**, VŠB Technological University of Ostrava, Faculty of Economics, Czech Republic
- **Vasiliev, Julian**, University of Economics in Varna, Bulgaria
- **Wielki, Janusz**, Opole University of Technology, Poland
- **Zaliwski, Andrew**, University of Auckland
- **Zhelezko, Boris**, Belorussian State Economic University, Belarus
- **Zhu, Yungang**, College of Computer Science and Technology, Jilin University, China
- **Zurada, Jozef**, College of Business University of Louisville, United States

ORGANIZING COMMITTEE

- **Hołowińska, Katarzyna**
- **Przysucha, Łukasz**, Wrocław University of Economics

Information Quality Challenges for the Preservation of Norwegian Public Sector Records

Markus Helfert
Dublin City University
School of Computing
Glasnevin,
Dublin, Ireland
Email: markus.helfert@dcu.ie

Petter Reinholdtsen
University Center for Information
Technology, University of Oslo,
Oslo, Norway
Email:
petter.reinholdtsen@usit.uio.no

Thomas Sødning
Oslo and Akershus University
College of Applied Sciences, Oslo,
Norway
Email: Thomas.Sodring@hioa.no

□ **Abstract**— The digitalization from paper-based to electronic records management results in challenges to preserve material in an authentic form. This paper explores the role in ensuring the authenticity and usability of electronic records in a long term preservation perspective. The discussion is viewed from an information quality perspective that provides a suitable lens to the topic. We identified a number of challenges that government records face, stressing the issue at hand of how to maintain authenticity and usability over a long term perspective. Challenges results from issues around authenticity, usability, the user, volume and heterogeneity and particular the time dimension. We conclude that the fields of record keeping and long term preservation have some clear information quality issues that could benefit from a concerted approach by integrating information quality research into records management. To date this seems to be missing.

I. INTRODUCTION

THE ongoing digitalization from paper-based records management to electronic records management challenges our ability to preserve material in an authentic form. Rubber stamps and signatures have been replaced with electronic signatures based on cryptographic principles and paper has been replaced by collaborative online word processing or reduced to semi-structured information stored in databases. This paradigm shift away from paper potentially allows government to be more cost effective as manual labor intensive processes are replaced by software. However it also introduces new challenges for content preservation, as the material that is amassed no longer has a physical form, rather it is often reduced to binary data unreadable or accessible by humans. This results in a significant challenge for records management and digital content preservation. The reason for this can probably be summed up in the following statement “I can easily pick up and read a book that’s 150 years old, but I cannot easily read the data stored on a tape that was connected to my

Commodore Plus/4 in 1985”. Technological obsolescence is an issue that challenges the ability to preserve electronic information.

This position paper focuses on two distinct professions working with government records, record keepers and archivists and is concerned with the process of extracting records from a relational database and depositing them with an archival institution. The results are an overview of our findings from a preliminary analysis of 12 years of government records from 1999 to 2012, for 5 various medium-sized Norwegian municipalities. The case-handling records were to be extracted a relational database adhering to the Noark standard. If we look at the digitisation process, there are many and various challenges that could be discussed. We have identified challenges emanating from an analysis of a number of databases containing electronic records when transferring records from the recordkeeping phase to the long term preservation phase. In this work we limit ourselves to challenges that became evident from our analysis, but there are other relevant challenges that could and should be identified and addressed. Another fact that complicates this discussion is that various countries have various approaches to record keeping and long term preservation, and as such the results may not be applicable to all countries.

The position we put forward for discussion is “*Information Quality has an important role in ensuring the authenticity and usability of electronic records in a long term preservation perspective*”

II. BACKGROUND

The domain of government records is all records that are generated from government action and governments have a duty and obligation to preserve such records [Public Records Act 1958]. At the state level, national tax and infrastructure planning are prime examples, while at municipal level, planning, local healthcare, transportation, child protection services etc. can exemplify government

□ This work was supported, in part, by Science Foundation Ireland grant 13/RC/2094 to Lero (www.lero.ie)

records. Very often these two levels of government interact and this interaction also produces records which also need to be preserved. In addition modern societies with complex tax and welfare programs will naturally generate more records than countries without such programs.

Government records are collected and subjected to long term preservation for evidential, legal, fiscal, informational or historical purposes [Schellenberg] and for an archive, achieving evidentiary value for its collections means maintaining authenticity and usability with a perspective that spans hundreds of years. With this in mind, a new challenge arises about the role that information quality could play with regards to the preservation of electronic records for a long time period, say in a 1000 year perspective. The field of Information quality has typically been concerned with the recordkeeping phase of electronic records and little work has been done on information quality from a long term preservation perspective [Conway 2011]. We have identified the following as relevant challenges that should be addressed when considering Information Quality and preservation: authenticity, usability, user, volume, heterogeneity and most important time.

III. CHALLENGES

A. *Authenticity*

One of the cardinal requirements for records is to maintain evidentiary value [Schellenberg]; to achieve this it must be possible to identify the authenticity of records. If a record is to be deemed authentic, it must be possible to prove that; the record is what it purports to be, that time elements (creation, dispatch, reception) are correct and involved individuals are identified correctly. Integrity is a property that is closely related to authenticity and often for a record to be deemed authentic it needs integrity. In this regard integrity can be defined as the degree of completeness of a record and whether or not we can prove record have been altered. Trust in records can be defined by whether or not we deem them as authentic. With paper, it is relatively easy to identify authenticity. Money is a very good example of this, where there are mechanisms in place so people know they can trust a monetary note as authentic.

How do we bring such trust mechanisms into play with electronic records? Typically, hashing [REF] is used on records and documents to determine if a record has been accidentally altered. That is a relatively, simple cheap and sufficient technique to determine integrity against bit rot or accidental changes to a record. Hash algorithms are also suitable for long term preservation as they are well documented and many implementations exist. It will not protect against willful modification of records, where both

the record and the hash is changed. As computers become faster, it might become computationally feasible to calculate how to change records and documents in a way that do not change the hash value. Hashing may solve part of the integrity issue but does not necessarily solve the authenticity issue. Hashing can solve authenticity if there are mechanisms in place to ensure we can trust the hash and original records. Documented processes, third-party logging of values, writing hash values to write-once-read-many media, trusted timestamping or writing hash values to a public blockchain are mechanisms to lift hashing from a integrity to a authenticity mechanism. Other approaches to authenticity include the use of public key infrastructure. Here an entity signs a hash of a record with their private key and their public key can be used to verify the signed record have not been changed. PKI may poses a particular challenge to preservation if the public key required to verify a signature is no longer available, or if the encryption mechanism has been broken to a point where it is computationally possible to create fake signatures. The public key is well know at the time it is used so the public key can easily be stored in relation to the record, but is only useful as long as the verification method is well known.

While the above points relate to individual records, dealing with large collections of records is also a challenge. Electronic records are typically stored in relational databases and it can be a challenge to preserve these over time. Just extracting database data as official records is a challenge and a natural question is quickly raised, How can we trust large database extractions? At the simplest level, one could create a database extraction as a backup and calculate a hash value for the extraction. This approach is common, but also naive. Who produced the extraction and how? Have all schemas been extracted, have the correct schemas been extracted?

Assuming authenticity without an understanding of usability is naive and dangerous and should be considered an information quality challenge.

B. *Usability*

In order to achieve usability, we must maintain storage, readability and understandability. If we are unable to store the information, we have lost it. Sometimes problems relating to storage are as simple as the fact that the people involved are not aware the data in a database is to be preserved and assume that once it is no longer in active use it can be deleted. When it comes to readability, an issue can be that a database backup extraction is seen as valid archival object. This can be problematic as the software to read the contents may fall away. This is a particular issue with databases from the eighties and early nineties. We know today that this issue is real and there are many examples of digital content that have been lost [OAG]

because we are simply no longer able to read the information. The municipality of Oslo for example has over 666 [OAG] various systems running on various database platforms. Preserving all of these databases is a challenge.

The SIARD file format (Software Independent Archiving of Relational Databases) is an interesting approach to this problem and solves the readability issue by converting the data in a relational database to a similar structure in XML. This data can then be imported back to a database for re-use, but also can act as a preservation object.

However, using relational database extractions as a preservation object has run foul of data privacy laws in Norway. The reason for this is that if it is not possible to identify records in the extraction, then it is not possible to be in compliance with data retention and disposal laws. A similar issue with readability is related to the use of older document file-formats. In particular document formats from the 80s that can no longer be interpreted and displayed by software is a challenge. While this issue is often over exaggerated as being a unsolvable problem, the authors did run into particular problems converting Lotus WordPro (lwp) files to PDF/A. The authors also had difficulty dealing with a variant of WordPerfect files stored in a database from eighties where the original frontend system likely had integrated fields for the automatic generation of documents and accurate reproduction of the document was not possible without the front-end system. This issue is one that can have a negative impact, not just on usability, but can also increase preservation costs significantly. The archive may have to preserve multiple versions of a document, instead of just an archive (suitable for long term preservation) version. The original version must be kept and examined when a user requests access to its contents. However at some point in the future, the tools to access the underlying data in such a document may no longer be available. In the case of the lwp files we examined, we were able to open them with a text editor, and even though there was some binary information there, a lot of the text was retrievable.

When it comes to understandability, a difficult issue to deal with is what is known as semantic drift. This is a result of the material being 'frozen' at the time it is archived, but society and the language we use evolves, slowly, over time. Over longer periods of time, this can have a major impact on understandability. If we consider records written in the 16 century in old English we know that the language used since then has evolved and this challenges both readability and understandability. It may be difficult for a layperson to read documents written in gothic script and even if you could read such documents you may not be in a position to

understand the contents as the English language has evolved.

It is difficult to imagine the effect that globalization will have on languages and how many of today's languages will still be around in 500 years, but this is something an archive must be aware of. But even within a language, there can be many dialects and sayings that will ultimately be lost. A major information quality challenge is how records survive the test of time and be available for users.

C. The user

When we talk about the notion of a user, we should picture the grandchildren of the grandchildren of the grandchildren of our children. That is the perspective we need to have. Within information quality, the user is often a guiding factor for research [Wang and Strong 1996], but for government records, in a preservation perspective, the idea of a user is sometimes secondary as the material is often preserved because of law, not because a user wants to interact with it. The OAIS model [CCSDS] argues the need for a clear definition of a designated community must be defined for archival collections; however, we see that in practice, the designated community is often an afterthought and as such the notion of a user is very open. Who will the user of electronic records in fifty years or five hundred years be? Humans will most likely access the material for personal and research reasons, but also artificial intelligence stemming from research into big data will probably be developed to create an understanding on why society evolved the way it did.

A natural question to ask is whether or not we are capturing enough information for future needs and to identify the level of quality of the information we are capturing. When records were paper based, it was easy to identify them, read them and process related information like comments written on paper. When records became electronic, we lost the ability to integrate a "human aspect", the handwritten note, or the extra related piece of information that has no place within an electronic system. It is likely that we are simply throwing information away because systems became digital. But we do not know for sure.

Collecting and centralizing large amounts of records related to a user can pose sensitivity challenges. For example, a person requesting a copy of a school diploma may find it uncomfortable when the archivist searches through their records and sees that the person has been sexually abused by a teacher. Another examples is where a user comes across information that might damage the psychologically. Perhaps a psychiatrist has asked for information not to be disclosed as the person is liable to self-injury if the person discovers such information. There is a need to balance access to information both in terms of

today's users but also users in the future. Relevant examples here can be seen in the release of archival records relating to criminal proceedings dating back one hundred years. Some family members report embarrassment when they find out their great grandmother was arrested for prostitution. Similarly, in 2011 nude pictures of the arctic explorer Fridtjof Nansen were released. He had taken pictures of himself that he sent to his wife. These two examples show that even though archive material is static, the story about the material evolves and can evoke feelings long into the future.

D. Volume and heterogeneity

The heterogeneity of data sources that government both create and use mean that archival institutions need to understand database structures of potentially thousands of systems. With the current trend of big data [Laney 2001] the challenges can be expected to increase [Haug and Arlbjørn 2010]. The municipality of Oslo, for example, has 666 various systems [OAG] containing digital information about citizens that should be preserved. Within these systems you will find a variety of databases and document formats that are no longer in daily use. Compounding this issue is a rapid technological evolution that gradually introduces obsolescence over time as volume continually increases. From our studies, we see that recordkeeping institutions typically have a focused time-frame over records. This act likes a window into the records and covers mostly all on-going cases. Case files from years back are seen as more archival in nature and data quality issues are not that important. There appears to be a need to limit the view of records, to keep the volume down. The problem with volume comes to light when you need to extract the records after 12 years. If you have 12 years of problems, incorrect data entry, bad system design, the you will have problems with preservation. These problems need to be identified and resolved.

Heterogeneity of material is also a matter for concern. The more the heterogeneity in file formats and database structures, the more difficult and costly preservation becomes. It becomes difficult to create a coherent understandable extraction, but also costly for the archive institution to preserve. Many archives have guidelines with regards to what file-formats they will accept and it may be difficult for the records creator to be in compliance. If they for example have 2 million documents in 20 different file formats and versions of file formats, it is difficult to guarantee the conversion process. Here heterogeneity and volume cross each other creating an additional challenge.

E. Time

Time is a challenge not only because of the long period of time records are to be preserved, but also because it results in changes in technology and society and these have an

effect on how we create, store and manage records. Time flows in one direction, nothing can stop that and if we do not address this challenge, we are creating digital mess that will be difficult to clean up. The term "technical debt" is often used to highlight the fact that an organization has hidden costs when dealing with the preservation of records. In the same way some argue that records are strategically important to an organization and should be managed as an asset, the mismanagement of records should be seen as a liability.

When it comes to preservation, time is both a challenge as well as a factor that compounds the other challenges. Over time, heterogeneity in the material and volume naturally increases along with technological evolution. Heterogeneity over time must be reduced by standardisation. We see this today with the use of the migration strategy for long-term preservation. As this is a cost issue, it is likely the archives will be forced to increase homogeneity.

The user and user expectations follows a similar trend with time, the technological evolution has given a new rise to user expectations of what an archive should deliver, today's generation will be impatient and have little understanding that archives cannot simply publish information. The user of tomorrow is likely to be based on big data /AI. Perhaps such algorithms will have a higher tolerance to bad information quality than humans do.

When it comes to usability, time is the very essence of semantic drift, but also a factor in the technological evolution that results in technological obsolescence.

At face value it would appear likely that authenticity mechanisms, like hashing, will not be affected by time. The hash, the data and the algorithm are all constant so there is little chance errors could occur. However bit-rot could be an issue on magnetic media, as a single flipped bit due to deteriorating media will cause a negative outcome when undertaking a hash check. Technology advancements might see concerted efforts to hack documents assumed safe by hashing. In much the same way bitcoin mining today attempts to create hashes, which follow a given pattern, we might find that future archive documents are subjected to attacks where the content of documents are replaced by malicious content with an equivalent hash. This could be achievable by inserting dummy non-visible data into e.g. a PDF file and mining the dummy data until the file hash matches the hash of the original file. While such an attack vector is unlikely with today's technology, as technology advances, the possibility may increase. Multiple hashes, using various algorithms, for each document is an easy way to reduce this attack vector.

The same argument could be made with PKI, that mining could be a potential problem, even though it is not one today. It is possible to store the original data, the public key that verifies the data and the algorithm to that

undertakes the verification process, in the same way that hashing is used today. In Norway, we know that this is not practice.

Almost paradoxically, one can observe that, time is an issue that can have a negative impact on long term preservation.

IV. DISCUSSION AND COUNTERARGUMENT

The position we argue is that “Information Quality has an important role in ensuring the authenticity and usability of electronic records in a long term preservation perspective”.

Information Quality is a mature and proven research field that has clearly made inroads to the field of record keeping. Its role in long term preservation is unclear though. The fields of recordkeeping and long term preservation are sometimes understood to be distinct, and that records exist in their own phases [Cunningham]. We believe this is the wrong view to have for records. Rather than solely focusing on issues within a single phase of a record, we should make information quality an overarching goal between the various phases. We need to understand the individual information quality needs during both recordkeeping and preservation. However when it comes to preservation, we can only inherit the inherent quality of the material and have little room to change anything. Fixing poor quality from the preservation phase is often so expensive, so fixing it becomes practically impossible, and as such any solution to preservation information quality must have its roots in the record keeping phase. However not all record keepers see preservation as their responsibility, so achieving acceptance for preservation information quality can be difficult.

To argue the other side of the position seems counter intuitive, that information quality has no role in ensuring authenticity and usability of electronic records. Of course it does, but approaching this from an information quality perspective may not be the only valid approach. A lot of research has been carried out in various disciplines that the archival profession has successfully used to push their own professional requirements. From the perspective of long term preservation, there is a need to bridge the gap between record keeping and long term preservation and using a formal information quality approach to bridge the two is worth exploring. We argue the need to pursue a more holistic approach to recordkeeping and long term preservation that finds its roots in the field of information quality.

We discussed the notion of a window into the electronic records. Such a window is a view of the records, where

individual record are clearly defined and relevant information quality measurements can be readily available. The first course of action must be to figure out what such window would look like. How do we create a window into what is arguably a very dynamic, distributed and ever changing architecture. Initial experimentation would suggest such a window must become larger than a time span of weeks to months and cover all records, or the window must become very narrow and focused and only move when high information quality is achieved.

V. CONCLUSION

We identified a number of challenges that government records face when dealing with the process of records going from active use to long term preservation, where the issue at hand really is how to maintain authenticity and usability over a long term perspective. Our case is guided by some preliminary work on information quality on government records and we see the need for more research on this topic, that there is no one-size fits-all solution and the archival profession must aim to achieve understandability and just readability of records.

The challenges described above are cross disciplinary and fall within a number of disciplines. Some may argue that such issues are resolved, and perhaps at an abstract level they have been discussed within an academic context, but to the best of our knowledge there have been no studies on the information quality issue when looking at the process of extracting records from a record keeping system and transferring the records to an archive that cover the information quality requirements of the archive. The fields of record keeping and long term preservation have some clear information quality issues that could benefit from a concerted approach by integrating information quality into their respective fields and to push information quality as an overarching issue that ties the two fields together.

ACKNOWLEDGMENT

This work was supported by the Business Informatics Group at Dublin City University and in part, by Science Foundation Ireland grant 13/RC/2094 and co-funded under the European Regional Development Fund through the Southern & Eastern Regional Operational Programme to Lero - the Irish Software Research Centre (www.lero.ie).

REFERENCES

- [1] Arnon Rosenthal, Len Seligman, and Scott Renner. 2004. From semantic integration to semantics management Case studies and a way forward. *ACM SIGMOD Rec.* 33, 4, 44–50.
- [2] Cinzia Cappiello, Francalanci, C. and Pernici, B., 2004. Time-related factors of data quality in multi-channel information systems, *Journal of Management Information Systems*, 20(3), pp. 71-91.
- [3] Mouzhi Ge, Helfert M, 2008. Data and Information Quality Assessment in Information Manufacturing Systems *Business Information Systems*,

- Volume 7, Lecture Notes in Business Information Processing (2008), pp 380-389.
- [4] Anders Haug, Arlbjørn J.S. 2010. Barriers to master data quality, *Journal of Enterprise Information Management*. Vol. 24 No. 3, pp. 288-303
- [5] CCSDS Secretariat, Space Communications and Navigation Office, 7L70. (2012). Reference Model for an Open Archival Information System (OAIS). Washington, D.C: UNT Digital Library.
- [6] Cunningham, A. (2008). Digital Curation/Digital Archiving: A View from the National Archives of Australila. *The American Archivist*, 71(2), 530-543
- [7] Dimitry Karagiannis, Mayr H., Mylopoulos J, 2016. Domain-Specific Conceptual Modeling, Springer.
- [8] Doug Laney (2001), '3D Data Management: Controlling Data Volume, Velocity, and Variety', Technical report, META Group .
- [9] OAG. Office of the Auditor General of Norway: investigation of the efforts to secure and make accessible archives in the municipal sector. Oslo: Riksrevisjonen 2010. Document 3:13 (2009-2010)
- [10] Public Records Act 1958. Available at <http://www.legislation.gov.uk/ukpga/Eliz2/6-7/51/contents> (Accessed: 30 August 2016).
- [11] Schellenberg, T. R. (1956) *The Appraisal of Modern Public Records*
- [12] Stuart E. Madnick, Richard Y. Wang, Yang W. Lee, and Hongwei Zhu. 2009. Overview and framework for data and information quality research. *ACM J. Data Informat. Qual.* 1, 1, Article #2.
- [13] Richard Y. Wang, 1998), A product perspective on total data quality management, *Communications of the ACM*, 41(2), pp. 58-65.
- [14] Richard Y. Wang, and Strong, D.M. (1996), Beyond accuracy: what data quality means to data consumers. *Journal of Management Information Systems*, 12(4), pp. 5-34.
- [15] Conway, Paul: Archival quality and long-term preservation: a research framework for validating the usefulness of digital surrogates *Archival Science*, November 2011, Volume 11, Issue 3, pp 293–309

Knowledge Management in The Cloud Computing Model - Challenges, Opportunities and Risks

Artur Rot, Malgorzata Sobinska
Wroclaw University of Economics,
ul. Komandorska 118/120,
53-345 Wroclaw, Poland
Email: {artur.rot,
malgorzata.sobinska}@ue.wroc.pl}

Abstract— With the increasing globalisation, the models for running business are changing as well, thus increasing the need for innovative knowledge management. This is facilitated by the development of information and communication technologies, which are the basis of numerous innovative solutions in the field of knowledge management. This article draws attention to the current trend in the area of IT management associated with the emergence and greater use of cloud computing. The article is an attempt to assess the impact of cloud computing on the key areas of knowledge management. It presents the challenges faced by organisations which place the emphasis on improving their competitive position, the possible positive consequences of the implementation of cloud solutions, as well as risks stemming from the use of clouds in the context of knowledge management.

I. INTRODUCTION

THE organisations that want to meet the emerging requirements and challenges of the market need to manage knowledge with particular skill, whereas the management should be tailored to individual needs and capabilities, as well as strategic objectives of the company. Knowledge management strategy should be based on three fundamental pillars: people, technology and processes [5]. Its implementation requires the integration of knowledge management processes with the strategic objectives of the organisation and business processes, operations in the social dimension - concerning the values and good practices cultivated in this area, and the provision of tools (modern technologies) necessary for the effective management of resources and knowledge processes. The experience of companies shows that success in knowledge management is achieved by the organisations which skillfully combine activities in each of these areas. Mere possession of knowledge and experience does not guarantee high efficiency.

In the article, the attention will be focused on the third dimension, i.e. the technology, which – despite not being the only or even the most important part of knowledge management – is nowadays a prerequisite for the successful

functioning of the company in the reality of global competition.

Organisations based on knowledge must create very specific and sophisticated information environment where information processes run using the most advanced information technology, covering both hardware and software [4, p. 15]. Companies are not always able to meet these challenges alone, therefore they frequently use external knowledge sources and external IT resources, resorting to, among others, various technologies for efficient functioning on a competitive market.

A study conducted on a group of companies operating in Poland shows that companies use various forms of sourcing for IT services. As many as 91% of the respondents admitted to the use of IT outsourcing, while 26% use cloud computing, and 13% prefers offshoring services [13]. The popularity of the use of cloud computing is also confirmed by research conducted among providers of cloud computing, system integrators, and users of cloud services [15, p. 279]. Other studies conducted by Cloud Connect and Everest Group from 2014 carried out on a group of 214 companies from around the world have shown that most organisations treat cloud computing as a strategic differentiator enabling operational excellence and accelerated innovation, in other words, they recognise the proposed value of the implementation of cloud solutions [12].

The main aim of this article is to attempt to assess the possible impact of cloud computing on the key areas of knowledge management. It will focus on both the potential positive and negative effects of the implementation of cloud solutions and the conditions under which the use of the cloud is worth considering.

The article is based on the analysis of literature and the results of the author's own empirical research involving interviews with employees of the IT departments in randomly selected organisations.

II. CHALLENGES FOR KNOWLEDGE MANAGEMENT IN MODERN ORGANISATIONS

The practice of knowledge management, whose importance was first recognised by leading organisations over twenty years ago, is now regarded as an integral part of management in almost every business organisation. The use of knowledge management processes increases the efficiency of decision-making processes as well as the level of operational efficiency, flexibility and the involvement of employees.

Globalisation is forcing organisations to adopt new styles of conducting business. Extended supply chains require more coordination through measures such as management of relationships with suppliers, management of internal processes, and management of customer relationships. Effective management of these elements requires significant changes in business strategies and encourages the use of new technologies [6]. The constant development of technology, in turn, causes the processes in enterprises to become more complicated, due to which the company is not always able to satisfy the requirements associated with owning, acquiring and developing the appropriate resources, including skills, knowledge and qualifications.

Increasingly, enterprises establish cooperation on the basis of various types of relationships, alliances, relationships, joint network-based forms of cooperation (e.g. logistic networks and production networks). There is a change in the location of knowledge and core competencies, which shift to the network, which in turn affects the changes in relation to innovation as a process based on competence. The novelty is the participation of consumers in the process of innovation and the use of their personal experience with the use of products or services as a rich source of ideas, which happens thanks to the highly-developed information technologies. From the position of the creator of innovation, the company moves to the position of the executor of the created innovation together with the consumer (e.g. through crowdsourcing), or partner – for example through cloud computing [11 p.17-19].

III. SERVICES OF KNOWLEDGE MANAGEMENT IN THE CLOUD

Cloud computing has great potential to provide knowledge management services in the following areas: improving decision-making processes, improving profitability, reducing the response time for critical problems of growth: productivity, market share, share prices, and competitive advantage.

Three basic models of cloud computing: IaaS - Infrastructure as a Service, PaaS- Platform as a Service and SaaS – Software as a Service can help organisations develop new models of knowledge management, collaborate with other organisations and facilitate the exchange of knowledge [1]. Cloud computing, according to M. Rafiq et al. not only provides an excellent location to manage data, information

and knowledge, but also provides a platform that can be used to make them available on demand, as well as other resources (networks, servers, storage, applications and services). Among the benefits of the integration of cloud computing with the system for knowledge management, there are: cost reduction, adaptation of new practices, discovery of new business models, and providing knowledge as a service (KaaS – Knowledge as a Service) [6]. S. Khoshnevis and F. Rabeifar propose the use of cloud technology to provide knowledge management, which can be widely used within the framework of business intelligence and competitive intelligence. Currently, these possibilities are not used for intra- and inter-organisational knowledge management systems. The authors illustrate the architecture of KMaaS (Knowledge Management as a Service) along with detailed services and associations and the relations between them. They also analyse how different cloud models can be used for knowledge management in the cloud environment and predict their application scenarios [3].

From the viewpoint of the “cloud’s” availability, it can be divided into the following categories [11, p.98]:

- *private* (internal);
- *common* (social);
- *public*;
- *hybrid*.

S. Khoshnevis and F. Rabeifar examine the relationship between the use of these models and the access to knowledge (explicit and quiet/hidden). Table 1 presents this relationship by referring the access to a specific type of knowledge for each of the cloud models.

TABLE I.
ACCESS TO KNOWLEDGE IN VARIOUS CLOUD MODELS

Type of cloud	Explicit knowledge	Hidden/quiet knowledge
Private cloud	Local/limited	Local/very limited
Public cloud	Very big	Extremely big
Social (common) cloud	Shared/limited	Shared/unlimited

In the case of private cloud, the access to explicit and hidden knowledge is local and limited to the organisation that owns the cloud. The launch of KMaaS in a private cloud seems to have a minimal impact on the knowledge management system, as it practically coincides with the local system of knowledge management. By contrast, the implementation of KMaaS in a public cloud looks very different. In this case, there is a high level of access to knowledge, both explicit and hidden, and it is particularly high in relation to the hidden knowledge, as it naturally belongs to a larger number of users (human minds) which use public cloud resources.

Social clouds are shared between specific organisations. In the case of access to the explicit and hidden knowledge, the access is neither as limited as in a private cloud, nor as

wide and open as in a public cloud. Hidden knowledge in this model is more readily available for the same reasons as the ones mentioned above with respect to a public cloud. The level of access to knowledge in hybrid solutions is difficult to investigate and depends on a combination of clouds hosted by the hybrid cloud.

Another point of the analysis pertains to the access to domain knowledge, depending on the location of the cloud - whether the cloud is owned by the organisation (whether it is "inside" the organisation) or is located on the "territory" of another organisation (outside) (Table 2).

TABLE II.
ACCESS TO DOMAIN KNOWLEDGE IN VARIOUS CLOUD MODELS

Type of cloud	"Inside" area	"Outside" area
Private cloud	limited/local organisational knowledge	Inaccessible
Public cloud	limited/local organisational and technological knowledge	unlimited inter-organisational external organisational/technological/marketing knowledge
Social (common) cloud	limited/local organisational and technological knowledge	limited inter-organisational external organisational/technological/marketing knowledge
Hybrid cloud	limited/local organisational and technological knowledge	limited/unlimited inter-organisational external organisational/technological knowledge

Private clouds offer limited local organisational knowledge, but do not give access to external knowledge. External clouds provide cross-organisational knowledge from all three areas (organisation, marketing, technology), while private clouds provide local intra-organisational knowledge. Public clouds provide unlimited access to knowledge, whereas social clouds provide limited access to knowledge, as well as hybrid clouds, which do not always provide permanent access to knowledge. Moreover, internal clouds (public and hybrid) can provide limited access to a maximum of two areas of expertise: organisational and technological [3].

The third point of the analysis refers to the degree of access to knowledge (explicit/hidden) in different cloud models. The level of access to both kinds of knowledge is low when using the private cloud. Public clouds allow wider access to knowledge, while the range of hidden knowledge is greater. Social clouds predict low or medium level of access to the two types of knowledge, whereas it is more difficult to analyse the level of access for hybrid clouds, which are a combination of all other types of clouds – they are usually estimated at the secondary level (Table 3).

Knowledge management can use cloud computing in two ways. Firstly, thanks to cloud computing, it adapts to

TABLE III.
ACCESS TO KNOWLEDGE IN VARIOUS CLOUD MODELS

Type of cloud	Explicit knowledge	Hidden knowledge
Private cloud	low	low
Public cloud	high/medium	high
Social (common) cloud	medium/low	medium
Hybrid cloud	medium (mixed)	medium (mixed)

technological advances, and secondly, it has the means which facilitate the exchange and acquisition of knowledge in a highly scattered and dynamic environment. Internet technology gives the possibility to build sophisticated, well performing knowledge management system designed to deliver content, from multiple sources, to each individual, in the individual's specific context and under the individual's own control. This ability helps to improve the relationship between knowledge/information/data suppliers and consumers by providing both parties more precise control over the interaction. Cloud technologies allow for a certain kind of controlled relationships between public, private, social, and hybrid clouds. In such a space, there is a facilitated creation of modern, network and virtual business models, which on the one hand require constant access to knowledge, and on the other hand supply and share vast amounts of valuable knowledge by themselves, which generates the need for a controlled exchange of knowledge between them.

IV. THE POTENTIAL AND RISKS OF CLOUD COMPUTING IN THE CONTEXT OF KNOWLEDGE MANAGEMENT

Organisations would like to benefit from the benefits of a "cloud" tailored to their needs, and the choice of a specific type is usually dictated by the size of the organisation, the scale of its activities, the willingness to take risks, and the investment opportunities [11, p. 99].

The benefits of a "cloud" are, among others: scalability, high availability, high performance, reliability, simplified management, flexibility. Thanks to these characteristics, cloud solutions can be regarded as a kind of accelerator for changes in the IT area, but like any new technology, they carry some risks [7].

According to IDC report, the market of data processing in cloud computing is currently the fastest growing part of the Polish market of information exchange [2]. Rapidly changing modern technologies offer great advantages, but, unfortunately, they also bring with them new forms of risk, making the traditional approach to information system security inadequate to the present situation. There constantly arise new types of risks, often misunderstood and underestimated by the management of the organisation [9]. The main risks, similarly as in the case of the classic outsourcing of IT services, include: loss of control over the

TABLE IV.
THE BENEFITS AND RISKS OF IMPLEMENTATION OF CLOUD COMPUTING IN SELECTED AREAS OF KNOWLEDGE MANAGEMENT,
OWN WORK

Areas/objectives of knowledge management	The potential of cloud computing	The risk associated with the implementation
Strategy/development of knowledge and competence resources	Access to external expertise, the latest technology; providing tools to enable access to organisational and technological knowledge; providing tools for support of the transfer and sharing of knowledge.	Loss of control over the IT environment; Dependence on the suppliers of cloud services.
Human resources management/ development of intellectual capital	Relieving the staff of the technical aspects and focusing on the core business activity; Developing new skills and competences in the field of IT; Improved cooperation and transfer of knowledge between organisations.	Possible loss of intellectual capital in case of the dismissal of IT staff as a result of the adaptation of cloud solutions; The loss of the capacity needed to return to self-provided IT services.
Process management	Supporting innovation; Reducing the time of process implementation.	
Marketing/business intelligence/innovation	Possibly unlimited access to internal and external knowledge. Ensuring the possibility of direct integration of external entities with the company; Supporting market-driven innovation (for products/services).	The possibility of losing competitive advantage by acquiring strategic information or sensitive data by the competitors.
Information technology/Information security management	Improved use of IT resources, high scalability of IT resources, availability, performance and reliability; Easier management, greater flexibility of IT infrastructure; Increased security thanks to advanced data protection tools used by service providers.	Loss of control over the IT environment; System failures; Services unfit for the actual needs of the organization; The decrease in safety (in the case of suppliers having weaker security systems); The possibility of loss and/or unauthorised use of sensitive data.

IT environment, failure of the mechanisms separating multi-tenants, risk of the loss of regulatory compatibility, insufficient data protection, the possibility of dependence on suppliers and the inability to return to self-provided IT services [8].

Table 4 presents the key risks and opportunities of cloud computing in respect of the areas and objectives of the “classic” knowledge management.

Proper management of the relationship with the cloud service provider can minimise some of the risks [9]; it also allows to standardise the variable IT environment in the cloud, reduction of operating costs and the achievement of comprehensive business knowledge. However, it requires a strong commitment on the part of managers, who must be capable of error-free evaluation of the current potential of IT, and anticipate the needs in order to not only take advantage of current opportunities, but also those that will appear in the next few years in the context of cloud computing. Cloud computing is in fact a platform for six other technologies, the combination of which, as experts predict, will have a huge impact on the future operation of the enterprises. They are as follows [14]: processing associated with the mobile Internet, automation of

knowledge-based works, robotics, Big Data, Internet of Things (IoT), and production based on 3D technology.

In the face of such an accelerated technology development, maintaining technological capacity within the organisation is critical, among other things, as a basis for the use of constantly growing outsourced IT and cloud computing services. It is also necessary to carry out technological changes in the organisational context in order to achieve a substantial and sustainable competitive advantage.

V. CONCLUSION

This article will serve as a starting point for more detailed research and analysis both in the purely technological area (e.g. regarding the mechanisms associated with the acquisition, processing or distribution of information; information security, etc.), and the “soft” area – e.g. a study of the impact of the adoption of cloud solutions for: managing the IT area, shaping the relationship between business departments, project management etc.

To sum up the above-mentioned considerations, one can come to the following conclusions:

- Proper management and transfer of knowledge within the organisation and in the relationship with the environment,

which is conducive to the development of IT, is vital to the survival and development of the organisation;

- Cloud computing can be a tool to support knowledge management and thus facilitate the growth of the efficiency of the IT departments and other units. It can become a valuable tool for access to and sharing of knowledge in the inner space of the organisation and in relations with other actors;
- Cloud computing can affect innovation services, processes, and even create new business models, and thus contribute to the improvement of the competitive position of companies that will adopt it skillfully.

In the complex and turbulent economic conditions, it is impossible to efficiently and effectively implement knowledge management processes without adequate support from increasingly advanced technology. In a situation where competition forces organisations to race against time, only the use of appropriate technological tools can improve (and sometimes even allow) the implementation of certain processes in the area of knowledge management [5].

It is, however, important to note that IT is only one of the three pillars of knowledge management. Today, information technologies are a prerequisite for the functioning of companies on global, highly competitive markets, but they cannot become the sole focus of knowledge management.

REFERENCES

- [1] Afshari M., "Cloud-Based Knowledge Management", 2016, <http://cloudtweaks.com/2014/06/cloud-based-knowledge-management/>, (accessed: 28.04.2016).
- [2] IDC, "Polski rynek usług w chmurze wzrosł o 25 proc. w 2015 r", *Puls Biznesu* <http://www.pb.pl/4275592,70326,idc-polski-rynek-uslug-w-chmurze-wzrosnie-o-25-proc-w-2015-r>, (accessed: 12.09.2016).
- [3] Khoshnevis S., Rabeifar F., "Toward Knowledge Management as a Service in Cloud-Based Environments, International Journal of Mechatronics", *Electrical and Computer Technology*, Vol. 2(4), July 2012, pp 88-110, ISSN: 2305-0543, <http://www.aeuo.org> (accessed: 26.04.2016).
- [4] Kozminski A. K., "Wstep", D. Jemielniak, A.K. Kozminski (eds.), *Zarządzanie wiedza*, Wydawnictwa Akademickie i Profesjonalne, Warsaw, 2008, pp. 7-16.
- [5] Mierzejewska B., "Czym (nie) jest zarządzanie wiedza", *E-mentor* 1 (3) / 2004, pp. 37-39.
- [6] Rafiq M., Bashar A., Shaikh A., "Innovative Trends in Knowledge Management: A Cloud Computing Perspective", *Proceedings of the First Middle East Conference on Global Business, Economics, Finance and Banking* (ME14 DUBAI Conference) 2014, http://globalbizresearch.org/Dubai_Conference/Conference_Papers.php, (accessed: 26.04.2016).
- [7] Rot A., "Enterprise Information Technology Security: Risk Management Perspective", *Proceedings of the World Congress on Engineering and Computer Science 2009*, Vol II, 2009, pp. 1171-1176.
- [8] Rot, A., Sobinska, M., "IT security threats in cloud computing sourcing model", M. Ganzha, L. Maciaszek, M. Paprzycki (eds.) *Proceedings of the 2013 Federated Conference on Computer Science and Information*, PTI, Cracow, <https://fedcsis.org/proceedings/2013/pliks/fedcsis.pdf> (accessed: 28.10.2016).
- [9] Rot A., „Zarządzanie ryzykiem w cyberprzestrzeni - wybrane zagadnienia teorii i praktyki”, T.M. Komorowski, J. Swacha (eds.), *Projektowanie i realizacja systemów informatycznych zarządzania. Wybrane aspekty*, Polskie Towarzystwo Informatyczne PTI, Warsaw 2016.
- [10] Sobinska M., "Sourcing usług i procesów informatycznych jako czynnik wzrostu innowacyjności organizacji", *Management Science* 4(21)/2014, ISSN 2080-6000, Wrocław University of Economics Publishing House, Wrocław, pp. 75-85.
- [11] Sobinska M., *Przewodnik sourcingu IT*, Wrocław University of Economics Publishing House, Wrocław 2015.
- [12] Sobinska M., Butryn B., „Cloud computing a transformacja roli działów IT”, *Przegląd Organizacji* 8(907)/2015, TNOiK journal, pp.32-38.
- [13] Sobinska M., Willcocks L.P., "IT outsourcing management in Poland - trends and performance", *Strategic Outsourcing: An International Journal*, Vol. 9/2015 Issue No. 1, <http://www.emeraldinsight.com/doi/full/10.1108/SO-10-2015-0024> (accessed: 19.09.2016).
- [14] Willcocks L., "How are we doing on cloud? Nine insights from leading global organizations", *Professional Outsourcing Resources*, 2016, <http://www.professionalloutsourcingmagazine.net/insight/how-are-we-doing-on-cloud-nine-insights-from-leading-global-organizations>, (accessed: 8.04.2016).
- [15] Willcocks, L. P., Lacity M. C., 2012, "The new IT outsourcing landscape. From innovation to cloud services", Palgrave Macmillan.

Software Systems Development & Applications

SSD&A is a FedCSIS conference area aiming at integrating and creating synergy between FedCSIS events that thematically subscribe to the discipline of software engineering. The SSD&A area emphasizes the issues relevant to developing and maintaining software systems that behave reliably, efficiently and effectively. This area investigates both established traditional approaches and modern emerging approaches to large software production and evolution. Events that constitute SSD&A are:

- IoTM'17 - 1st Workshop on Internet of Things, Process Modelling and Microservices
- IWCPs'17 - 4th International Workshop on Cyber-Physical Systems
- LASD'17 - 1st International Conference on Lean and Agile Software Development
- MIDI'17- 4th Conference on Multimedia, Interaction, Design and Innovation
- SEW-37 - The 37th IEEE Software Engineering Workshop

4th International Workshop on Cyber-Physical Systems

PROLIFERATION of computers in everyday life requires cautious investigation of approaches related to the specification, design, implementation, testing, and use of modern computer systems interfacing with real world and controlling their surroundings. Cyber-Physical Systems (CPS) are physical and engineering systems closely integrated with their typically networked environment. Modern airplanes, automobiles, or medical devices are practically networks of computers. Sensors, robots, and intelligent devices are abundant. Human life depends on them. Cyber-physical systems transform how people interact with the physical world just like the Internet transformed how people interact with one another.

The event is a continuation and extension of 2006-2010 Real-Time Software FedCSIS workshops and 2013, 2015, 2016 IWCPSS. The objective of the workshop is to serve the community with main interest in CPS.

The workshop will accept papers in the following areas:

- Control Systems
 - real-time/embedded/networked
 - wireless sensing/actuation
 - process control & cloud computing
- Internet of Things
 - system organization/implementation
 - device security
 - impact on business
- Scalability/Complexity
 - modularity
 - design methodologies
 - legacy systems
 - tools
- Interoperability
 - concurrency
 - models of computation
 - networking
 - heterogeneity
- Validation and Verification
 - safety assurance & certification
 - simulation
- Cyber-security
 - intrusion detection
 - resilience
 - privacy
 - attack vectors
- Applications of CPS
 - intelligent measurements in medicine, environment, etc.
 - robotics, manufacturing
 - intelligent/autonomous cars
 - transportation, ITS
 - power systems including smart grids
 - smart cities
 - military
 - smart consumer devices
- CPS Education
 - curriculum development
 - on-line and virtual laboratories
 - academic courses
 - pedagogy issues

SECTION EDITORS

- **Grega, Wojciech**, AGH University of Science and Technology, Poland
- **Kornecki, Andrew J.**, Embry Riddle Aeronautical University, United States
- **Szruc, Tomasz**, AGH University of Science and Technology, Poland
- **Zalewski, Janusz**, Florida Gulf Coast University, United States

REVIEWERS

- **Babiceanu, Radu**, Embry Riddle Aeronautical University, United States
- **Bianchini, Devis**, Università degli Studi di Brescia
- **Čaplinskas, Albertas**, Vilnius University, Lithuania
- **Černohorský, Jindřich**, VSB Technical University of Ostrava, Czech Republic
- **Cicirelli, Franco**, Università della Calabria, Italy
- **Cosulschi, Mirel**, University of Craiova, Romania
- **Ehrenberger, Wolfgang**, University of Applied Science Fulda, Germany
- **Friesel, Anna**, Technical University of Denmark, Denmark
- **Furht, Borko**, Florida Atlantic University, United States
- **Giurca, Adrian**, Brandenburg University of Technology, Germany
- **Golatoski, Frank**, University of Rostock, Germany
- **Gomes, Luis**, Universidade Nova de Lisboa, Portugal
- **Greitans, Modris**, Institute of Electronics and Computer Science, Latvia
- **Grosu, Radu**, Technische Universität Wien, Austria

- **Gumzej, Roman**, Faculty of Logistics, University of Maribor, Slovenia
- **Haverkort, Boudewijn R.**, University of Twente, The Netherlands
- **Laplante, Phillip A.**, PennState University, United States
- **Letia, Tiberiu**, Technical University of Cluj-Napoca, Romania
- **Majstorovic, Vidosav D.**, University of Belgrade, Serbia
- **Marwedel, Peter**, Technische Universität Dortmund, Germany
- **Monostori, László**, Hungarian Academy of Sciences, Hungary
- **Motus, Leo**, Tallinn University of Technology, Estonia
- **Nalepa, Grzegorz J.**, AGH University of Science and Technology, Poland
- **Obermaisser, Roman**, Universität Siegen, Germany
- **Roman, Dumitru**, SINTEF / University of Oslo, Norway
- **Rozenblit, Jerzy W.**, University of Arizona, United States
- **Rysavy, Ondrej**, Brno University of Technology, Czech Republic
- **Sachenko, Anatoly**, Ternopil National Economic University, Ukraine
- **Saglietti, Francesca**, University of Erlangen-Nuremberg, Germany
- **Sanden, Bo**, Colorado Technical University, United States
- **Sanz, Ricardo**, Universidad Politecnica de Madrid, Spain
- **Schagaev, Igor**, London Metropolitan University, United Kingdom
- **Selic, Bran**, Simula Research Lab, Norway
- **Sojka, Michal**, Czech Technical University, Czech Republic
- **Sveda, Miroslav**, Brno University of Technology, Czech Republic
- **Trybus, Leszek**, Rzeszow University of Technology, Poland
- **van Katwijk, Jan**, Delft University of Technology, The Netherlands
- **van Lier, Ben**, Rotterdam University of Applied Sciences, The Netherlands
- **Vardanega, Tullio**, University of Padova, Italy
- **Veža, Ivica**, University of Split, Croatia
- **Villa, Tiziano**, Università di Verona, Italy
- **Waeselynck, Hélène**, LAAS-CNRS Toulouse, France
- **Zlatogor, Minchev**, Bulgarian Academy of Sciences
- **Zoebel, Dieter**, University Koblenz-Landau, Germany

Industrial Use Cases of Cyber Physical Systems in EU Projects: Preliminary Study

Rima Al-Ali

Abstract—Smart Cyber-Physical Systems, introduced by Horizon2020, are the foundation of Industry 4.0 due to the communication between collective intelligent physical devices. Since the usage of sCPS spans over plenty of domains facing variety of challenges, it becomes rather difficult to select an appropriate representative case study for demonstration of approaches developed in research. In this paper, we present a systematic review of sCPS case studies that allows us to identify the domains addressing similar challenges and quantify some of their properties. We group the industrial use cases according to their challenges and map them to the domains.

Index Terms—Cyber-Physical Systems, Survey, Demonstrator, Use Case, Application.

I. INTRODUCTION

DEMONSTRATORS, or use cases, are an important tool to illustrate research questions and validate developed ideas, methods, and solutions. Having suitable examples is crucial for demonstration of research results. Moreover, potential variety of domains that the research tackle prove their generality and reusability. Even though the challenges differ across different projects, naturally, they are fixed on a particular one.

Hence, when aiming at development of a “general” method that would be easy to compare with related ones, it is hard to select the right use case for the purpose of presenting and validating. To achieve that, the researchers need to go to the details of each single use case (taken from a selected set) bearing in mind that knowing the domain does not help much in this task. Another option would be to have a predefined use case from an industrial partner, which could limit the method and the solution to be domain-specific.

On the other hand, from the industrial point of view, presenting reusable methods and solutions just in some domains different from theirs makes it harder to match the possibility of applying this particular method on the applications they already have.

Smart Cyber-Physical Systems (sCPS) [10] are interesting for both academic and industrial communities due to the wide range of their applications. The sCPS are introduced in Horizon2020 calls as up-and-coming systems that consider dynamicity within systems involving communication between physical and computational parts known as cyber-physical

systems. In fact, CPSs are considered the foundation of the Industry 4.0 [14], which introduces wireless communication between the embedded devices in manufacturing, aiming at decentralized decision making during a production process.

The current surveys and systematic reviews mostly target CPS architectures (i.e., decomposition into smaller parts and their interconnection) and their applications, which is a well-known method to deal with the increasing complexity of those systems.

This includes various aspects, such as Architectural Description Languages (ADL) [16] (called architectural languages (AL) in the paper) and self-adaptation [7], as well as many others [15] [12] [11]. For instance, in [17], the authors are interested in identifying the application domains, challenges, goals, and solutions of architecting CPSs. The systematic study found links between challenges and the suggested solutions for architecting CPSs, which provided a clear idea as to what kind of research could be targeted in the future. In contrast to this, the researchers in [7] headed for finding out application domains and uncertainty types in self-adaptive CPS, and they were able to synthesize patterns from multiple adaptation mechanisms and identify on which layers of the CPS architecture they are applied. As a result of this study, the patterns present an engineering method to be used in designing future self-adaptive CPS.

Regardless of the application domains, in an industrial study [16], the authors raised questions related to the use and the need of ADLs in industry. In this survey, the authors prepared a questionnaire and asked the experts to fill it or made interviews with them. Interestingly, although the ADLs have many domain-specific concepts, the industrial experts consider them very general. However, the study concluded that the needs of industries were not fulfilled by academic ADLs, which highlighted the gap between academic and industrial interests. However, to our best knowledge, no studies involve matching the domains of the collective behavior use cases to their challenges on CORDIS database. Hence, the main goal of this position paper is to present preliminary results on identifying the relations between the demonstrator domains and their challenges. Furthermore, the paper describes an initial grouping of use cases depending on their challenges, which provides other researchers with a wider range of options in choosing an appropriate demonstrator in terms of both the domains and

The paper is submitted for review on 31/5/2017. This research is partially supported by ICT COST Action IC1404 Multi-Paradigm Modelling for Cyber-Physical Systems (MPM4CPS) of the H2020 program.

Rima Al-Ali is a PhD student at Department of Distributed and Dependable Systems, Mathematics and Physics Faculty, Charles University, Prague, Czech Republic (alali@d3s.mff.cuni.cz).

challenges.

This paper is organized as follows: Section 2 presents the systematic review, while Section 3 presents the results of the study. Section 4 describes our plans for future work and concludes the paper.

II. THE SYSTEMATIC REVIEW

To minimize any bias in our research, we decided to perform a systematic review to collect relevant demonstrators for our study. We followed the guidelines of Kitchenham for performing Systematic Literature Reviews in Software Engineering [13]. We briefly summarized the guidelines here to make it easier to follow our steps.

The guidelines start with explaining the need for the systematic review. At the beginning, the researchers have to define the *research questions*, which the review is expected to answer. In case they would like to know the type and the amount of research, they are heading for *systematic mapping review*. On the other hand, in case the researchers are experts in a specific area and they seek for more details about the current state of the art, they should take advantage of *systematic literature review*. The next step is to develop a *review protocol*, which is a document that includes all systematic review steps and is sent to the reviewers for evaluation. The study has to clarify the *source of primary studies*, e.g., source: scholar search engines, primary studies: conference papers.

Then, the researchers have to list *inclusion* and *exclusion criteria* to be applied on the primary studies. Not only do these criteria help in focusing the results and minimize the number of resulted primary studies, but also they ensure getting the same results if anyone else re-does the review using the same set of primary studies. Moreover, the researchers should define the *study procedures*, which describe how the selection study is performed. Both study criteria and procedures must have quality assessments to evaluate the sensitivity and the limitations of the study.

From the discovered primary studies, the researchers extract the data needed to address the research questions using data extraction forms. Further, they synthesize the knowledge they are heading for from the data, which is the final result and potentially a subject to dissemination. Of course, the systematic review protocol should include all the information previously acquired in addition to a timetable of the study tasks for the reviewers.

Therefore, following the guidelines in Fig. 1, we start with an overview of our interests in the study.

A. Background

The requirements for our study have real industrial use cases that target smart Cyber-Physical Systems (sCPS). In this regard, we focused on three basic parts of sCPS: smartness aspect, collective aspect, and physical aspect.

1) Smart Aspect

This part represents the smartness in the system, its ability to perform self-adaption, and make decisions depending on the context.

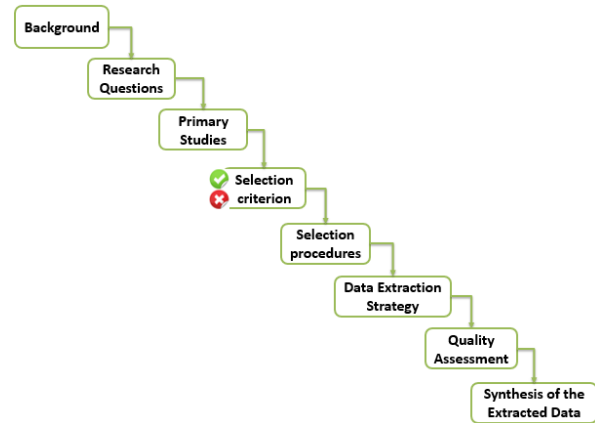


Fig. 1. Systematic Literature Review Steps

2) Collective Aspect

This part represents the collective behavior inside the system where many entities communicate with each other and are involved in forming distributed system behavior, such as in case of Internet of Things (IoT).

3) Physical Aspect

This part considers hardware devices that interact between each other, such as sensors and actuators.

B. Research questions

The research questions are defined to help in grouping the use cases depending on their challenges. Our study is driven by the following research questions:

RQ1: What are the typical domains for the collective sCPS use cases?

RQ2: What are the principle challenges addressed by the use cases in collective sCPS?

C. Search for primary studies

As industrial use cases are our focus in this study, we decided to target the use cases of European projects with Industrial Leadership. The calls that provide such projects (in alignment with our CPS interest) are Information and Communication Technologies (ICT) calls.

Needless to say that the quality of the European projects is high due to all the processes of projects evaluation. In addition, the proposals of the projects have a mandatory requirement to reach high Technology Readiness Level (TRL) [6], which should reach TRL6; this ensures having a working (physical) demonstrator as a requirement for accepting a project proposal. It is worth mentioning that beside the project indicated requirements, we also searched in CORDIS [8] for CPS projects and most of the found projects were accepted under ICT calls, which shows that it the best target for our study.

We considered the projects in the past 10 years as a sample of recent results in this area of research. Therefore, we end up with targeting FP7-ICT and Horizon2020-ICT calls [1] [2] [3] [4] [5] [6]. The calls for FP7 range from 2007 to 2013 and in H2020 from 2014 to 2016. However, since the projects under H2020

that started in 2016 are still without results, we have not included them in the review.

Of course, the database is trustworthy since it is from CORDIS on European Commission website, which is the main information source about the European projects.

D. Study selection criteria.

We defined four basic criteria that correspond to the interests of our study. As listed in TABLE I, each of the first three criteria contains a set of representative keywords, which we require to be included in the call and project description. In fact, these keywords are extracted manually from a sample of highly related calls and projects description, and then we filter them to obtain a more representative set.

We include the primary studies (projects) that satisfy all the following constraints (i.e., *Inclusion Criteria (IC)*):

IC1: Call was made in 2007 – now.

IC2: Call title has at least one keyword from at least one of the criteria of the first three ones.

IC3: Call description has one keyword at least from each criteria of the first three ones.

IC4: Project title has at least one keyword from any criteria of the first three ones.

IC5: Project description has at least one keyword from each criteria of the first three ones.

IC6: Project has deliverables, reports or a demonstrator description.

IC7: Challenges of the use cases target collective behavior.

IC8: Use cases have more than two interacting entities, which represent the collective behavior (e.g., many robots work together, many robots interact with humans)

We exclude the projects (i.e., *Exclusion Criteria (EC)*) according to the following exclusion criteria:

EC1: Call started 2016-2017 since it is without results yet (i.e., no periodic report).

EC2: Call description contains only keywords in context different from one of the three first criteria (e.g., collaboration between researchers).

EC3: Project description contains only keywords in context different from one of the three first criteria (e.g., collaboration between researchers).

EC4: Project does not have working website.

EC5: Project has no deliverables, reports nor a demonstrator description.

EC6: Use case challenges are unrelated to collective behavior.

EC7: Use cases represent a collective knowledge exchange between people (e.g., social networks, software for rating places, roadmaps, and platforms).

EC8: Use cases have one-to-one or one-to-many relation between robots and human (e.g., wearables, tour guide robot).

E. Study selection procedures.

The selection procedures are presented in four basic parts: primary studies, calls, projects, and use cases.

TABLE I
SELECTION CRITERIA

Criteria 1 Smart aspect	Criteria 2 Collective aspect	Criteria 3 Physical aspect	Criteria 4 Entities
smart(*)	distribut(*)	physical	# > 2
intelligen(*)	de(-)central(*)	CPS	
adapt(*)	co(-)operat(*)	Internet of Things	
autonom(*)	communicat(*)	IoT	
aware(*)	collaborat(*)	embedded	
	connective(*)	device	
	emergent	hardware	
	swarm	robot	
	collective		

(*) means zero or several letters

(-) means it is possible to contain hyphen in the word

means number of entities or nodes that interact in use case

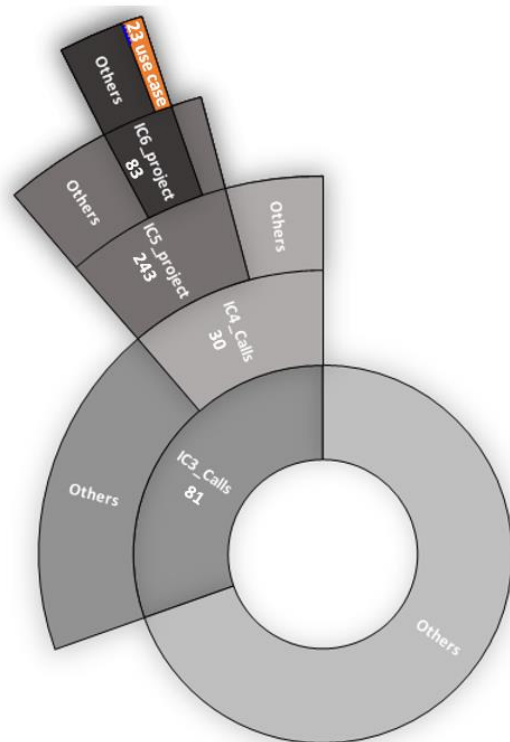


Fig. 2. The Selection of Use Cases – The Final Set in Orange

The first part is related to the study foundation, and the procedure follows the guidelines in [13]. Therefore, we started with: (1) describing the background of the research interest, followed by (2) defining the research questions. Afterwards, (3) we selected the calls of Information and Communication Technologies (ICT), which are FP7 and Horizon2020 [9] calls from 2007 to 2016 as a target [IC1]. Next, (4) we defined four criteria out of which three are the sets of keywords (i.e. see TABLE I).

The second part is related to selection of ICT Calls, where (5) we looked up for any of the keywords in the title of the calls [IC2], (6) excluding the 2016-2017 calls since the corresponding projects do not have results on the website yet [EC1]. Afterwards, (7) we searched in the resulted calls description for at least one keyword from each criteria [IC3] [EC2]. Then, from the final filtered calls, (8) we created a report containing the all the projects.

The third part is related to project selection, which starts with (9) looking up for any of the keywords in the title of the projects [IC4]. Then, (10) in the resulted projects, we looked up for each project description that contains at least one keyword from each criteria [IC5] [EC3]. Further, (11) we filtered out the projects that are without a working website [EC4]. In case that the website in CORDIS does not work, we looked up for the website using the “(project title) + project” as the search string in Google. Then, (12) we selected the projects that had documentation for their demonstrators as a description in the website, deliverables, or reports [IC6] [EC5]. Finally, (13) from the final set of projects, we created a list of all corresponding use cases.

The fourth and the last part is related to selecting the use cases. Here, (14) we select the use cases with challenges that target collective behavior [IC7][EC6][EC7]. After that, (15) we selected the use cases that are designed for more than two nodes [IC8][EC8].

F. Study quality assessment checklists and procedures.

This part requires having an evaluation from reviewers, which we still miss as this work is still in progress. However, we plan to have the study reviewed by at least two experts. Nevertheless, in the future work section below, we discuss the sensitivity and the quality of our study that is affected by many points, such as the selection of the primary studies, the selection of the keywords sets, the evaluation of collective challenges, and the evaluation of the number of nodes.

G. Data extraction strategy

We have used pre-defined extraction forms (i.e. see TABLE II, TABLE III, TABLE IV). Each table contains basic information that is needed to apply the selection procedures. Therefore, we defined a form for all calls, which required the title, the description of the call, and the criteria 1|2|3 fields that hold the extracted data from the project descriptions. Similarly, the second form is related to the project data, which includes the title, the description, website availability, and the criteria 1|2|3 fields. The last form contains use cases information, which consists of use case description, its domain, its challenges, the number of its nodes, and its documentation availability. Finally, the targeted data to address our research questions is in the “Use Case Domain” and “Use Case Challenges”. The former one is related the RQ1, while the latter is related to RQ2.

III. RESULTS

After applying the method on all H2020 and FP7 calls, the results of research questions are extracted and further analyzed from the point of view of both domain and challenges fields. In the following sections, we present our results.

A. General Statistics

Fig. 2 describes the numbers of each selection procedures, which starts with total number 266 of the presented calls in both FP7 and H2020. After applying the selection procedure to calls using steps 1-8, the number of selected calls decreases to 30,

TABLE II
DATA EXTRACTION FORM FOR CALLS

Data Item – Call	
Call ID:	Call Title:
Call Description:	
Criteria1:	Criteria2:
Criteria3:	

“Call Description” is the text in ICT work program.

TABLE III
DATA EXTRACTION FORMS FOR PROJECTS

Data Item - Project	
Call ID:	Project ID:
Project Name:	Project Title:
Description:	
Criteria1:	Criteria2:
Criteria3:	
Website:	

“Project Description” is the text in CORDIS website.

TABLE IV
DATA EXTRACTION FORM FOR USE CASES

Data Item – Use Cases	
Project ID:	Use Case ID:
Domain:	Use Case Description:
Demonstrator:	Challenges:
Criteria4:	
Demonstrator Description (yes/no)	Deliverables and reports (yes/no)

“Use Case Description” is the description in the project website or in the deliverables. “Demonstrator” is an abstract of the use case description. “Challenges” is the abstract of use case challenges.

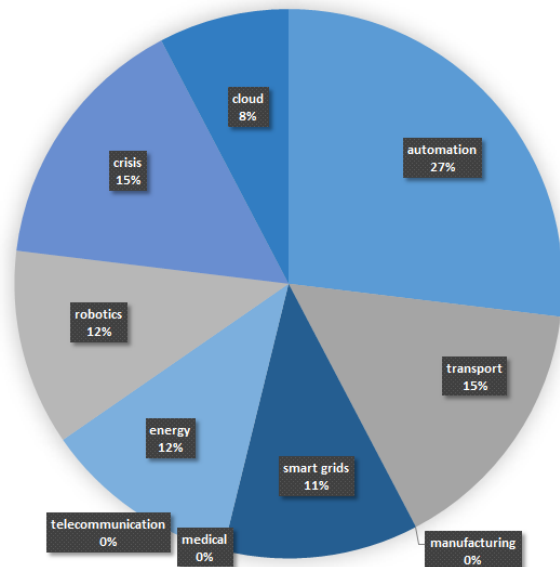


Fig. 3. Domains Percentage of the Selected Use Cases

which corresponds to 348 projects. Then, after applying steps 9-13, the number of the selected projects went down to 83, which corresponds to 96 use cases. Finally, after applying steps 14-15, the final number of selected use cases is 23.

B. Use Cases Domains (RQ1)

The domains of the selected use cases after applying selection procedures are: clouds, crisis, robotics, telecommunication, energy, medical, smart grids, manufacturing, automation, and transport (i.e. see Fig. 3). There is some overlap between those domains, but we related each use case to just one domain except for three use cases that stated multiple domains explicitly in

TABLE V
GROUPING CHALLENGES

Safety	Awareness	Uncertainty	Collective goal	Communication	Resources	Planning
overcome failure of individual	environment-aware	uncertainty in sensors data	reach inaccessible /wide areas	short range communication	sharing resources	
unexpected failure	dynamicity	unpredictable dynamics	achieve shared goal	limited communication	energy demand	
avoid obstacle	context-aware		helping elderly	lack of communication	trading resources	
recover failure	situation-aware		team goal	network problems	cost	
safety				delays	load distribution	
human safety					limited time	
					energy waste	
					energy efficiency	
					performance	
					traffic load	

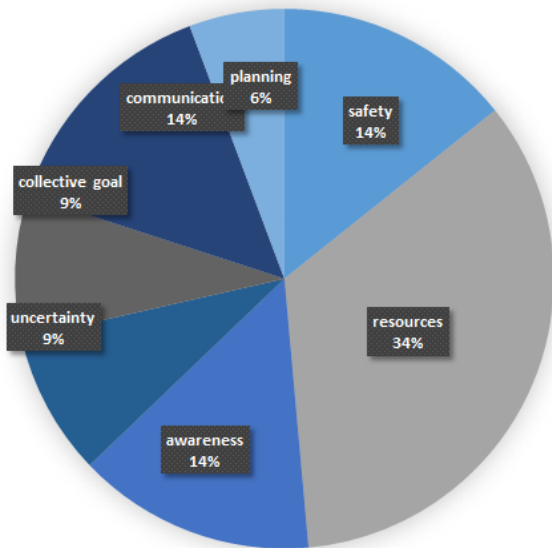


Fig. 5. Challenges Percentage in the Selected Use Cases

DOMAIN	projects	safety	resources	awareness	uncertainty	collective goal	communication	planning
Automation								
	VICINITY		✓					
	symbioTe	✓		✓				
	HYDROBIONETS				✓			✓
	SCUBA			✓				
	IPAC		✓					
Transport								
	VICINITY		✓					
	symbioTe		✓					
	ASCENS		✓					✓
Manufacturing								
Smart Grids								
	OrPHEuS		✓					
	INERTIA		✓					
	INTEGTIS		✓					✓
Medical								
Telecommunication								
Energy								
	VICINITY		✓					
	GreenCom		✓					
Robotics								
	CADDY	✓						
	RECONFIG	✓						
	EMICAB			✓				✓
Crisis								
	SHERPA	✓	✓	✓		✓	✓	
	NIFTI	✓	✓	✓		✓	✓	
	ASCENS	✓				✓	✓	
	IPAC							✓
Cloud								
	ClouT							✓
	ASCENS							✓
sum		5	12	5	3	3	5	2

Fig. 4. Mapping the Challenges to Use Cases Domain

their descriptions (the use cases are pilots of a smart city scenario).

The automation use cases cover various views of automation, such as building automation, railways and industry automation (e.g., home management, decentralized management of manufacturing entities), while in case of transport, the use cases target planning, and e-charging and sharing parking places. In case of crisis, the usual use case is having a team of collaborating robots and humans that aim at saving lives. Despite the fact that most of the robotics use cases focus on learning and better interaction with human, some of them involve groups of robots that aim at achieving a common goal collectively.

In case of smart grids and energy, both domains have the energy management scenario. For clouds, this involves performance and distributing load.

Most of the use cases in telecommunication were concerned with mobile applications for exchanging knowledge between people (e.g., social networking). As to the medical use cases, they focused on monitoring and developing specialized robots that helped elderly people or people in need (e.g., in the form of a wearable to keep the balance during walking). Regarding manufacturing, this domain contains developing and building the hardware more than using it in a collective use case.

As illustrated by the chart in Fig. 3, the answer of the first research question “RQ1: What are the typical domains for the

smart collective CPS use cases?” is “automation”, then “transport”, and “crisis”.

C. Use Cases Challenges (RQ2).

The challenges of the selected use cases after applying selection procedures are grouped into the following representative ones (TABLE V): safety, resources, awareness, uncertainty, collective goal, communication, monitoring, and planning (Fig. 5).

The resource group, which is the biggest one, targets any kind of resources such as time, energy, and cost. The safety group includes every challenge that corresponds to safety of the system or its entities including humans, in addition to safe recovery from failures. Further, awareness group targets a collective awareness of the environment and the context that surrounds the system entities for a better performance. Another important challenge group is communication; this group targets any problem that could happen with the communication in the system stemming from its limitations, failures or even a lack of it.

Even though collective goal groups are less addressed in our selected use cases, they form a significant part in CPS. More specifically, the system entities in CPS tend to be grouped in a decentralized way to achieve common goals that they are not able to reach alone or it is more costly. Although uncertainty exists everywhere inside and outside of a sCPS system, it is

explicitly targeted here in data uncertainty and situation unpredictability. It is worth mentioning that uncertainty also can be caused by delays, problems in networking, unexpected failures, and unexpected situations, which means it is involved in more than one group. Since we tried to have a reasonable representation for it, we introduced a separate group for it.

As illustrated in Fig. 4, the answer of the second research question “**RQ2:** What are the principle **challenges** addressed by the use case?” is resources, then safety, communication, and awareness.

D. Mapping Challenges to Domains

In Fig. 4, we matched the representative challenges of the selected use case to their domains. As a result, we notice that resources and communication as a challenges target most of the domains, Moreover, awareness as well as safety are very important to automation and crisis in addition to robotics domains since it is required to have a high level of realization to the surroundings due to its criticality and cost.

Surprisingly, the only domain where the collective goal is addressed is crisis, while planning gets the interest of transport and robotics domains; uncertainty are considered in automation and robotics.

To sum up, the resources and communication cover most of the domains, while there is a lack in addressing other challenges in transport, cloud, energy, and smart grids. Also, manufacturing, telecommunication, and medical domains are not represented well by industrial use cases of collective sCPS.

IV. CONCLUSION AND FUTURE WORK

Smart CPSs are spreading around with their possible applications in industries as well as in academic research. Therefore, we need a way to find out what challenges correspond to which domains in industrial use cases. For this reason, we did a systematic mapping review to find the domains and the challenges that industry targets nowadays. The primary studies that we used are EU projects from the ICT calls since 2007 until now.

The results of the study showed that the most targeted domain is automation and the most addressed challenge is resources. Moreover, domains such as transport, cloud, energy, and smart grids lack variety of challenges, while many other domains do not target any collective challenge. Those include telecommunication, medical and manufacturing domains.

As future work, we plan to validate the results and extend the study to contain academic use cases in the aim of comparing the difference in interests between industrial-based and academic-based use cases, regarding domains and challenges. Furthermore, we plan to synthesize a small set of representative use cases for the presented challenges to be used in case of presenting a general method instead of using a domain specific use case.

V. APPENDIX

In this appendix, we present in TABLE VI the list of project that contains the final selected set of use cases.

VI. ACKNOWLEDGMENT

This paper is partially supported by ICT COST Action IC1404 Multi-Paradigm Modelling for Cyber-Physical Systems (MPM4CPS) of the H2020 program. Additionally, I would like to express my thanks of gratitude to Tomáš Bureš, Jan Kofroň, and Lubomír Bulej, who helped me during my work.

TABLE VI
PROJECTS WITH SELECTED USE CASES

Project Name	Project Title
VICINITY	Open virtual neighbourhood network to connect intelligent buildings and smart objects Website: http://vicinity2020.eu/vicinity/
symblo	Symbiosis of smart objects across IoT environments Website: https://www.symbiote-h2020.eu/
CADDY	Cognitive autonomous diving buddy Website: http://caddy-fp7.eu/
OrPHEuS	OPTimising Hybrid Energy grids for smart cities Website: http://www.orpheus-project.eu/
ClouT	ClouT: Cloud of Things for empowering the citizen clout in smart cities Website: http://clout-project.eu/
SHERPA	Smart collaboration between Humans and ground-aerial Robots for improving rescuing activities in Alpine environments Website: http://www.sherpa-project.eu/sherpa/
RECONFIG	Cognitive, Decentralized Coordination of Heterogeneous Multi-Robot Systems via Reconfigurable Task Planning Website: http://www.reconfig.eu/
HYDROBIO NETS	Autonomous Control of Large-scale Water Treatment Plants based on Self-Organized Wireless BioMEM Sensor and Actuator Networks Website: http://www.hydrobionets.eu/
SCUBA	SCUBA - Self-organising, Cooperative, and robust Building Automation Website: http://www.aws.cit.ie/scuba/
GreenCom	MyGrid; Energy Efficient and Interoperable Smart Energy Systems for Local Communities Website: http://www.greencom-project.eu/
INERTIA	Integrating Active, Flexible and Responsive Tertiary Prosumers into a Smart Distribution Grid Website: http://www.inertia-project.eu/inertia/
EMICAB	Embodied Motion Intelligence for Cognitive, Autonomous Robots Website: http://www.emicab.eu/
NIFTi	Natural human-robot cooperation in dynamic environments Website: http://www.nifti.eu/
INTEGRIS	INTElligent Electrical Grid Sensor communications Website: http://fp7integriss.eu/index.php
ASCENS	Autonomic Service-Component Ensembles Website: http://www.ascens-ist.eu/
IPAC	Integrated Platform for Autonomic Computing Website: http://ipac.di.uoa.gr/

REFERENCES

- [1] European Commission. ICT work programme 2007/2008, FP7 EU projects. [Online]. Available: http://ec.europa.eu/research/participants/data/ref/fp7/88465/c-wp-200801_en.pdf, 2007
- [2] European Commission. ICT work programme 2009/2010, FP7 EU projects. [Online]. Available: http://cordis.europa.eu/pub/fp7/ict/docs/ict-wp-2009-10_en.pdf, 2009
- [3] European Commission. ICT work programme 2011/2012, FP7 EU projects. [Online]. Available: <http://cordis.europa.eu/fp7/ict/components/documents/ict-wp-2011-12-en.pdf>, 2011.
- [4] European Commission. ICT work programme 2013, FP7 EU projects. [Online]. Available: <https://cordis.europa.eu/fp7/ict/docs/ict-wp2013-10-7-2013-with-cover-issn.pdf>, 2013.
- [5] European Commission. ICT work programme 2014/2015, H2020 EU projects. [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/main/h2020-wp1415-leit-ict_en.pdf, 2014.
- [6] European Commission. ICT work programme 2016/2017, H2020 EU projects. [Online]. Available: http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-leit-ict_en.pdf, 2016.
- [7] A. Musil, et al., "Patterns for Self-Adaptation in Cyber-Physical Systems Multi-Disciplinary Engineering for Cyber-Physical Production Systems," *Data Models and Software Solutions for Handling Complex Engineering Projects*, Springer International Publishing, pp. 331-368, May 2017, doi: 10.1007/978-3-319-56345-9_13.
- [8] European Commission. Cordis. [Online]. Available: http://cordis.europa.eu/home_en.html
- [9] European Commission. Horizon 2020. [Online]. Available: <https://ec.europa.eu/programmes/horizon2020/>
- [10] European Commission. Smart cyber-physical systems, Horizon2020. [Online]. Available: <https://ec.europa.eu/programmes/horizon2020/en/h2020-section/smart-cyber-physical-systems>
- [11] D. Dac Hoang, H. Paik, and C. Kim, "Service-oriented middleware architectures for cyber-physical systems," *IJCSNS International Journal of Computer Science and Network Security*, vol.12, no. 1, January, 2012.
- [12] P. Derler, E. A. Lee, and A. Sangiovanni Vincentelli, "Modeling Cyber Physical Systems," *Proceedings of the IEEE*, vol.100, no.1, pp. 13–28, January 2012, , doi: 0.1109/JPROC.2011.2160929.
- [13] B. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering," *Technical Report, EBSE-2007*.
- [14] Y. Lu, "Industry 4.0: A Survey on Technologies, Applications and Open Research Issues," *Journal of Industrial Information Integration*, vol. 6, pp. 1-10, June 2017, doi: 10.1016/j.jii.2017.04.005.
- [15] C. A. Macana, N. Quijano, and E. Mojica-Nava, "A survey on Cyber Physical Energy Systems and their applications on smart grids," In 2011 IEEE PES Conference on Innovative Smart Grid Technologies Latin America (ISGT LA), pp. 1–7, October 2011, doi: 10.1109/ISGT-LA.2011.6083194.
- [16] I. Malavolta, et al., "What Industry Needs from Architectural Languages: A Survey," *IEEE Transactions on Software Engineering*, vol. 39, no. 6, pp.869–891, June 2013, doi: 10.1109/TSE.2012.74.
- [17] I. Malavolta, H. Muccini, and M. Sharaf, "A preliminary study on architecting cyber-physical systems," In *Proceedings of the 2015 European Conference on Software Architecture Workshops, ECSAW '15*, pp. 1–6, New York, NY, USA, 2015, doi: 10.1145/2797433.2797453.

Utilising Latent Data in Smart Buildings: A Process Model to Collect, Analyse and Make Building Data Accessible for Smart Industries

Zohreh Pourzolfaghar

Dublin City University, School of Computing
Dublin, Ireland
Zohreh.pourzolfaghar@dcu.ie

Markus Helfert

Dublin City University, School of Computing
Dublin, Ireland
Markus.helfert@dcu.ie

Abstract— Smart buildings are embedded with large amounts of latent data from different sources, e.g. IoT devices, sensors, and the like. Integration of this latent data with the buildings information can highly impact efficiency of the services provided by various industries, e.g. facility management companies, utility companies, smart commerce, and so forth. To manage buildings information, diverse technologies such as Building Information Modelling (BIM) technology have been developed and changed the traditional approaches. Notwithstanding a plethora of research in this area, potential users of this information, such as facility management companies, are still unable to fully benefit from the building information. This is due to the fact that various information and data have been heterogeneously scattered across various sources. To overcome this challenge, this research follows the design science approach to propose a process model to enable facility management industry to access the integration of buildings information with live data. The presented process model is introduced thoroughly by explaining the required steps to collect and integrate and preserve the integrated information and data. The evaluation of the process model was undertaken via the employment of a focus group session with the construction professionals, the IoT experts, and the data analysts. Also, this paper elaborates on two industrial use-cases to demonstrate how having access to the building information effectively affects the other industries. The outcome of this research provides an open access to the integration of building information and live data for diverse range of users.

Keywords— *building information management, data capture, IOT devices, sensors, building Information Modelling (BIM)*

I. INTRODUCTION

The smart buildings information is a valuable asset which can be utilised by various types of stakeholders in the smart cities, (e.g. by city councils for urban and infrastructure planning, maintenance/facility management companies to speed up their services and utility companies to estimate energy consumption). Smart building describes “a suite of technologies used to make the design, construction, and operation of buildings more efficient [28]. To enable smart buildings, [29] believed that a wider range of information should be available from a broader range of sources. The buildings information is generated during various stages of buildings life cycle. The first stage of buildings information

creation is the design phase. This information is mostly related to the buildings specifications, spaces, heating and cooling systems and their specification and so on. Numerous researchers described various advantages gained from such information. For instance, [6] stated that it is exceedingly important to have the capability of quickly and reliably estimating the buildings’ energy consumption, especially for public authorities and institutions that own and manage large building stocks. As Asadi [2] explained, estimating and predicting the buildings energy consumption depend on multiple variables like building characteristics, the energy systems characteristics. The operation phase is another stage of building life cycle in which new information is created. In this phase, the smart technologies, devices and sensors produce live data which can be utilized for the environmental monitoring applications [23] or for the combinational usage of different context data from different sources [8]. Likewise, combination of the live data with building information can provide priceless information for various potential users. For instance, live data on energy consumption for a building can be compared with the energy consumption estimation from the design phase. The results of this comparison can be utilized to promote energy saving behavior.

Despite of importance of this combination, many researchers reported challenges to take advantage from this combination. Some of these challenges are related to the vast complexity and volume of the data and information generated during the buildings’ life cycle [14], fewer advances in the information management methodologies and fragmented models in the construction industry [17], [21].

Moreover, buildings information is scattered across the separated data storages and in heterogeneous formats. As [1] proclaimed, these issues contribute to some other key challenges in terms of the manual driven process to utilise the buildings information, lack of proper quality control procedures, and obsolescence of the information.

With regard to the abovementioned challenges, this research proposes a process model with the aim of integrating the building information with the live data. In the subsequent parts of this paper, first we review some related research work in the building information management field. Then, a process

model is introduced as the proposed solution. The evaluation section includes four sub-sections to provide more details on the evaluation steps, including the focus group session, exploring the two use-cases, and discussion on the results.

II. RELATED RESEARCH WORKS

During the last ten years, the Building Information Modelling (BIM) technologies have become more common to manage the buildings information. However, these technologies confront large number of challenges, e.g. updated data for the as-built BIM models [4], the pertinent semantic format for the maintenance stage [22], unsystematic use of the building information on the virtual models [16], the related procedures [5], the established standards [10], and the computerised facility management system integration [3].

As such some researchers reported challenges facing the maintenance stage to benefit from combination of building information. For instance, [18] reported several corresponding obstacles in terms of availability the required data for maintenance stage and usability of the stored data format. As such [26] and [22] identified challenges relate to interoperability, interfaces with other systems, integration of wired and wireless sensor networks to enhance the live data collection during the construction phase, and controlling the access to the project information. Also, [15] proclaimed that the building maintenance requires a comprehensive information system that captures/retrieves the information about the building maintenance components and all their related building components. In this regard, they proposed an integrated information/knowledge system. However, this system was limited to capturing and retrieving the data during the maintenance phase.

The data integration was defined by [7] as: “the combination of data from different sources with unified access to the data for its users”. Apparently, many researchers proposed methods and models to integrate the building information with the live data to facilitate the maintenance of the buildings. However, inadequate data integration is a current challenge faced by the building information models. According to [18] this challenge stems from differences in the data syntax, the schema, or the semantics. With regard to the studied literature, integration of information and data has been recognized a challenge. To tackle this challenge, this research aims to present a process model to collect, analyse, and

integrate the building information with the live data captured from various IoT and smart devices and sensors.

III. RESEARCH APPROACH

This paper follows [19] the design science research approach to define the problem in terms of unavailability of a combination of the building information with the live data. To define the problem, related literature has been reviewed in the area of the technologies to manage the building information, e.g. the BIM. To support the problem in practice, the authors conducted meetings and workshops with the facility management teams as the potential users of this combination. Based on the evidences from the literature review and workshops with practitioners, the problem was defined as the inability to take advantage from the combination of buildings information with the live data. Therefore, this research proposed a process model to extract the buildings information and the live data from heterogeneous sources, then combine and store them in an open access storage. For the conceptual evaluation of the presented model, this study followed [25] to conduct a focus group discussion session. The focus group session passed through eight steps procedure [24], with the practitioners from the construction industry, the IOT experts and the data analysts. The results of evaluation provide evidences on relevancy of the proposed process model for the explored field.

IV. PROCESS MODEL FOR BUILDING INFORMATION AND LIVE DATA INTEGRATION

Buildings information is known as a priceless resource for various smart industries. For instance, utility companies can utilise building information to estimate energy consumption and promote energy saving [20]. For this purpose, they need the cumulative information of electrical devices, while detailed buildings information may not be accessible. Similarly, other industries such as retailers can predict and manage market demands with regard to the technical specification for building components and materials [20]. However, building information is not openly available for these typical potential industry users. To provide such an ability, the initial overall idea to integrate building information with live data, as well as making buildings information accessible for all potential users, is presented in Fig 1.

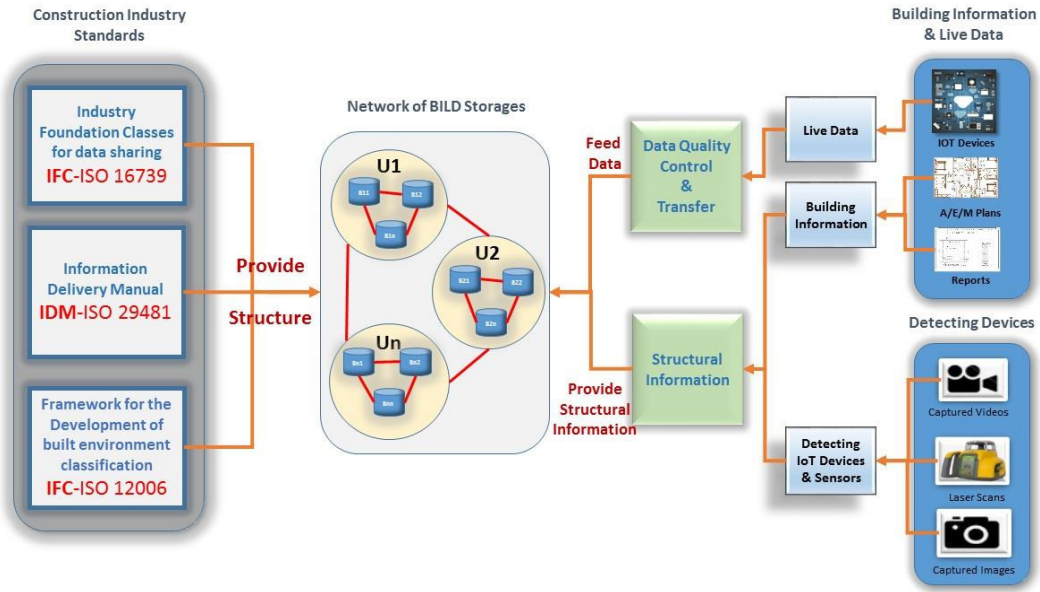


Fig. 1. The overall view of the Process Model

According to the diagram in Fig 1, buildings information and live data are extracted from various sources. The information and data are utilised for two different purposes, including: to define the structure of the storage; and to feed into the storage. The information and live data will feed into the storage after passing the quality control phase. Referring to the left side of the diagram, the existing construction industry standards (e.g. ISO 12006) for the information exchange should be considered to construct the storage. In the middle side, the network of BILD (Building Information & Live Data) storages is presented. Any storage (e.g. B11) is for one building in an urban area (e.g. U1). Also all the storages are connected to each other.

Establishing on this overall view, this study proposes a process model to capture the data from various source and integrate them into a Building Information and Live Data (BILD) open storage. Consequently, four phases have been defined for the proposed process model. In the following subsections, the above mentioned phases of the process model are described thoroughly.

A. Structuring BILD Open Storage

The first phase of the proposed process model is structuring the open storage in which integrated and qualified building information and live data are stored. The open storages structure should comply with the construction industry standards, (i.e. ISO 16739, ISO 12006, ISO 29481). To develop such an open storage, the first phase of the process model comprises the following steps. The first step is exploring Building Information Modelling (BIM) standards, (which are the European standards for the construction industry). Based on these standards, all the data should follow the corresponding rules. Based on the explored standards, some structural and semantical requirements are specified. Regarding these requirements, an initial version of the open storage structure is defined. Another important requirement for this phase is defining and standardising the coding system for building spaces. Later, the assigned codes are used to link the collected live data from various sources to the buildings information. The presented process for this phase is shown in Fig. 2.

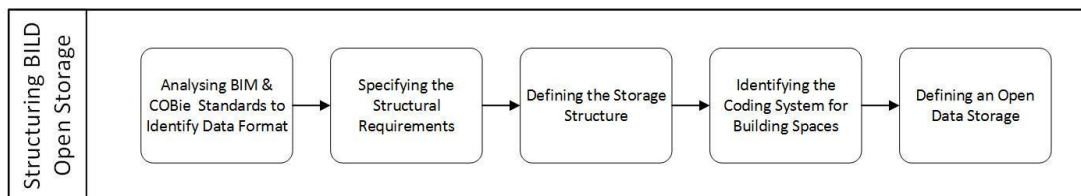


Fig. 2. The process of structuring BILD open storage

Structuring the BILD storage will be completed after accomplishing the second and third phases. This is due to the fact that the required fields to preserve the information and collected data are specified through the later steps.

B. Multi-sources Building Information Capturing

In this section the required steps to capture the buildings information from various sources (e.g. building plans, reports, IOT devices, sensors, etc.) are explained. To this goal, two different sub-processes are proposed in this section. The first

process is to digitalise building information from architectural/mechanical/electrical plans as well as project reports. Building plans contains essential information about building spaces and their associated technical specification. Likewise, project reports comprise useful information on mechanical/electrical/structural aspects, e.g. building energy consumption. As the first step for this process, all this

information is required to be digitalised. Then, the next step is using a coding system (defined in 4.1) to assign unique code to the building spaces. Later, there will be a need to provide a link between the digitalised building information from plans and from the project reports. This information is stored in the structured data storage in section 4.1. The defined process for this stage is shown in Fig. 3.

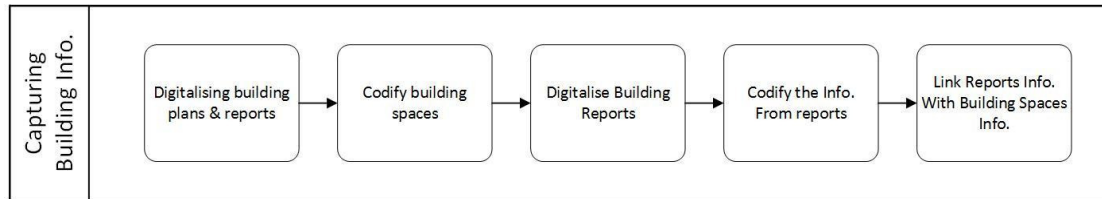


Fig. 3. The process of capturing building information from plans and reports

The second process for this stage is detecting all the IOT devices and sensors installed in the building spaces. This process is to update the information about the new installed devices in building space. To do so, all these devices are detected using laser scans, captured images and video records.

The outcome of the detecting devices is in the form of point cloud data and they need to be converted into the objects. Moreover, some additional information e.g. coordination and location are utilised to link this information to the previous building information. The second process is presented in Fig. 4.

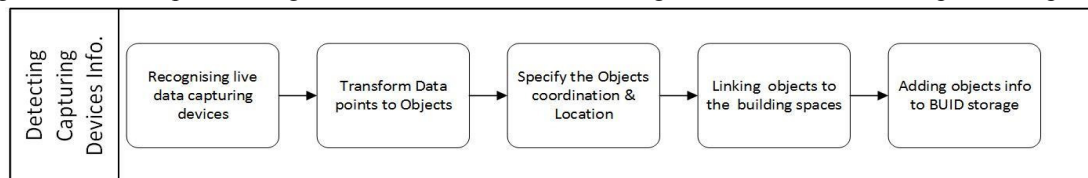


Fig. 4. The process of detecting IoT devices and sensors information

During this phase, some structural information is also provided to complete the structure of the data storage in phase 4.1. The iterative process of feeding live data into the BILD storage is presented later, in section D.

C. Establishing a BILD Storages Network

By providing a network of data storages for the buildings, an opportunity is arising to use integration of buildings information with live data for the urban planning purpose in smart cities (e.g. for infrastructure planning and waste water management based on energy consumption in an urban area).

To establish such a network, the required steps are explained as follows. In the first step of this process, locational information should be defined for the buildings. Then, a codifying system should be defined to develop and assign a unique code to every building in an urban area in the city. This unique code is the reference number for each building. In this regard, all the buildings in the urban areas could be referenced with their unique code. Finally, the required field for all the above mentioned information in this phase should be added to the storage structure. The proposed process for this section is presented in Fig. 5.

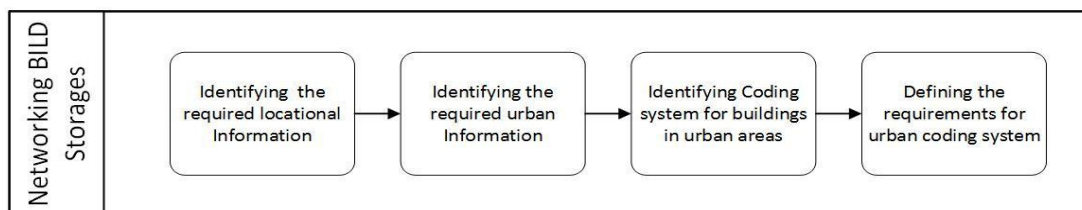


Fig. 5. The process building network of BILD storages

D. Multi-sources Live Data Capturing

The last phase of the proposed process model is transferring the qualified live data to the BILD storage. As the first step of this process, the live data is captured from the detected devices and sensor. The captured data from IoT and smart devices are stored in the database associated with their software. In this condition, there is a need to define an interface to obtain and

transfer this data to the BILD storage. Referring to the second phase (i.e. 4.2), some fields have been defined to store the live data for the installed devices in the building spaces. Therefore, the capture data can be transferred to their related fields in the BILD storage. However, before this step there is a need to ensure about the quality of the captured data. In case of passing the quality control step, data is ready to be transferred to BILD storage. This process is shown in Fig. 6.

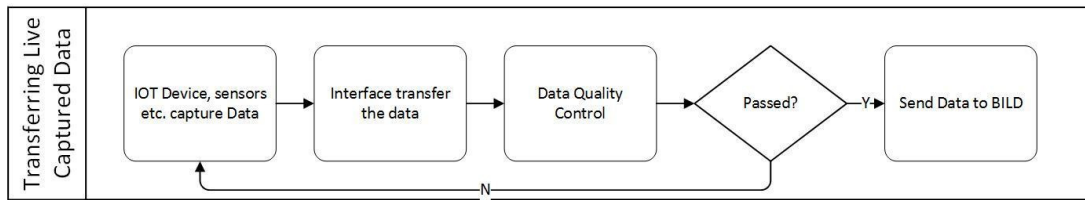


Fig. 6. The Qualifying and Transferring the live data to BILD storage

Indeed, this is the only iterative phase in the whole process model. This phase is responsible to provide the most updated data on the status of the installed devices in building spaces.

The abovementioned phases have been defined to collect, qualify, integrate and store building information and live data

in an open storage. This storage will be accessible by all industries. The relations between these four phases are shown in Fig 7.

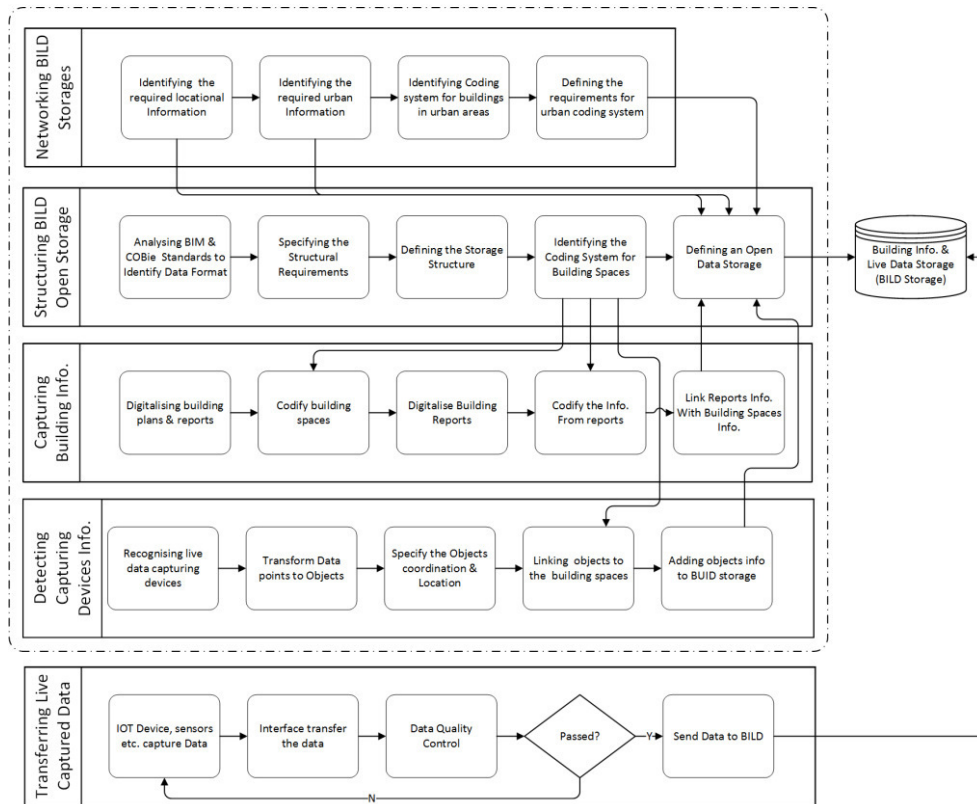


Fig. 7. The overall process model and relations between sub-processes

Based on the above process model, the defined sub-processes for four phases are interacting to build up the structure, as well as feeding the information into the BILD storage. The first four sub-processes in the process model are happening once (to construct the BILD storage structure), while the last phase is the iterative sub-process which continuously feed live data into the storage. Indeed, this phase is responsible to update the installed devices status. The proposed process model has been demonstrated to the experts in construction field, IOT devices and sensors for validation purpose. In the next section, more details are provided on the validation of the presented process model.

V. VALIDATION

For evaluation purpose of the presented process model, this research follows [25] ex-ante evaluation approach. To do this, first a focus group discussion was conducted for conceptual evaluation of the process model in terms of relevancy of the process model to the challenges in building information area. Later, two different use-cases are explained as the evidences to prove that this information are current in this field. In the following three sub-sections more details are provided on focus group discussion and two use-cases. Later, in the fourth sub-section, a discussion is conducted on two evaluation aspects, i.e. relevancy and if the information is current.

A. Focus Group Discussion with Professionals

According to procedure stated in [24], to apply focus groups in in the design science context, some steps are needed to be considered. The sequence of these steps are: 1) formulating the problem; 2) identifying sample frame; 3) identifying a moderator; 4) developing and pre-test a questioning route; 5) recruit participants; 6) conduct focus group; 7) analyse and interpret data; and 8) report the results. Based on these requirements, the question for the focus group session defined as: ‘whether the proposed model is relevant to the current challenges, (information and data integration), to manage building information’. The focus group attendees were six professional in the areas of construction industry, IOT and data analysis. This focus group session was conducted with the aim of providing some evidences from participants on how good this process model may fit into its defined goals. The main two goals of the process model are: 1) integration of building information and captured data; and 2) storing this information in an open access storage consistent with construction industry standards. The main objective for this session was getting a consensus on to how extend this process model may achieve its defined goals. Therefore, we invited two participants for each of three different areas in the process model, i.e. construction practitioners, IOT experts, data analysts. The moderator of the session was the main author of this paper who has a background in construction industry. For developing and pre-testing the questions, we first defined questioning route. For this purpose, this research followed [12] to conduct a conceptual evaluation. Then, we interviewed two invited practitioners and revised the questions based on their expertise. In the following two sub-sections two use-cases of using building information are described as the evidences for usefulness of building information to other smart industries. Then, in sub-section 5.4 the results of focus group session and two use-cases are discussed altogether.

B. Building Information and maintenance

As [9] believed, the proliferation of advanced computerisation throughout industry has revolutionised the way that buildings are designed, constructed, operated and maintained. According to [15] one of the key challenges in building projects is the need to have sufficient information on products ready available for any maintenance operation. Also [16] believed that maintenance information of products installed into buildings should be available for maintenance stage. Likewise [16] stressed that detailed product data might be needed to respond to the demands from authorities or users to track the used products. Apparently, there is a high demand for integration of building information with live data from IoT and smart devices in buildings. Therefore, the proposed process model by this study can be a solution for the recognised challenges for maintenance phase of buildings.

C. Building Information and Smart Energy

Regarding the increased efforts for energy saving and energy cost reduction, utility companies attempt to find new ways to promote more effective ways of energy usage. In this

regard, [6] emphasised on the importance of the capability to reliably estimate the buildings’ energy consumption. For this purpose, many researchers utilised machine learning and data mining [27], or regression models [11] to predict and estimate building energy consumption. Some other researches e.g. [13] and [2] stressed that estimation of building energy consumption highly depends on building information. While many researchers proposed methods to estimate and calculate energy consumption, there are valuable resources to provide this information. The energy consumption for buildings are estimated during early design phase of buildings. As such, energy consumption for buildings are measured and calculated by IoT and smart device. Combination of this information can provide responses to many concerns, e.g. comparing the energy consumption with initial estimation to promote energy saving behavior.

D. Discussion on Focus Group Results and Use-Cases

During the focus group session, four different questions related to four phases of the proposed process model were discussed. According to the results, all the participants believed that different phases of the process model are relevant and necessary for data integration. Also they all stressed that this information is sufficiently current in their area. For instance, IOT experts stated that this is a new demand from their customers’ side to have a list of IOT devices installed in the buildings and they are looking for a solution to respond to this need. Similarly, construction experts believed that the integration of live data with building information is an essential issue in this area. Therefore, they strongly believed that presented process model has the ability to address data integration issues. As a result of this evaluation session, all the participants believed that this process model is an appropriate and exact approach to respond the current demands in the construction industry. From the other side, two explored use-cases realised that other smart industries may benefit the integrated information. Therefore, these use-cases are evidences on this fact that building information is current for smart industries as well. Therefore, this study believes that the presented process model can provide smart industries openly access to the buildings information.

VI. CONCLUSION

The buildings information integrated with live data is a valuable asset which can be beneficial to many smart industries. Although diverse technologies such as building information modelling have been developed to manage the building information, however, industry users still are not able to take advantage from the combination of this information with the live data. Moreover, this combination should be openly accessible needless of the skills to use specific professional environments like the BIM. Overcoming this challenge, this research presented a process model to collect and integrate and store the integrated buildings information with the live data in an open storage. The presented process model by this paper has been prepared to apply in a real project in collaboration with facility management industry. By going through the future steps to implement the presented process model, more details will be provided to the readers.

ACKNOWLEDGMENT

This work was supported by the Science Foundation Ireland grant “13/RC/2094” and co-funded under the European Regional Development Fund through the Southern & Eastern Regional Operational Programme to Lero - the Irish Software Research Centre (www.lero.ie).

REFERENCES

- [1] M. Ajam, M. Alshawi, and T. Mezher, “Augmented process model for e-tendering: Towards integrating object models with document management systems,” *Autom. Constr.* Vol. 19, pp. 762-778, 2010. <https://doi.org/10.1016/j.autcon.2010.04.001>
- [2] S. Asadi, S. Shams Amiri, and M. Mottahed, “On the Development of Multi-Linear Regression Analysis to Assess Energy Consumption in the Early Stages of Building Design,” *Energy and Buildings*, Vol. 85, pp. 246-255, 2014. <http://dx.doi.org/10.1016/j.enbuild.2014.07.096>
- [3] B. Becerik-Gerber, F. Jazizadeh, N. Li and G. Calis, “Application areas and data requirements for BIM-enabled facilities management,” *J. Constr. Eng. Manag.* Vol. 138, pp. 431-442, 2011. [10.1061/\(ASCE\)CO.1943-7862.0000433](https://doi.org/10.1061/(ASCE)CO.1943-7862.0000433)
- [4] N. Gu, V. Singh, K. London, L. Brankovic, and C. Taylor, “Adopting building information modeling (BIM) as collaboration platform in the design industry, CAADRIA 2008: beyond computer-aided design,” *Proc. of the 13th Conference on Computer Aided Architectural Design Research in Asia, The Association for Computer Aided Architectural Design Research in Asia (CAADRIA)*, 2008.
- [5] British Institute of Facilities Management, (2013). “Benchmarking: Effective Performance Management for FM,” British Institute of Facilities Management, UK, 2013.
- [6] A. Capozzoli, D. Grassi, and F. Causone, “Estimation models of heating energy consumption in schools for local authorities planning,” *Energy and Buildings*, Vol. 105, pp. 302-313, 2015. <https://doi.org/10.1016/j.enbuild.2015.07.024>
- [7] I. F. Cruz, and H. Xiao, (2009). *Ontology Driven Data Integration in Heterogeneous Networks, Complex Systems in Knowledge-based Environments: Theory, Models and Applications*, Springer, Heidelberg, 2013, pp. 75–98.
- [8] A. D’Elia, L. Roffia, G. Zamagni, F. Vergari, P. Bellavista, A. Toninelli, and S. Mattarozzi, “Smart applications for the maintenance of large buildings: How to achieve ontology-based interoperability at the information level,” In *Computers and Communications (ISCC)*, IEEE Symposium, pp. 1077-1082, 2010. [10.1109/ISCC.2010.5546639](https://doi.org/10.1109/ISCC.2010.5546639)
- [9] C. Eastman, C. M. Eastman, P. Teicholz, R. Sacks, and K. Liston, *BIM Handbook: A Guide to Building Information Modeling for Owners, Managers, Designers, Engineers and Contractors*, John Wiley & Sons, Hoboken, 2011. (ISBN: 978-0-470-54137-1).
- [10] M. Kassem, G. Kelly, N. Dawood, M. Serginson, and S. Lockley, “BIM in facilities management applications: a case study of a large university complex,” *Built Environ. Project Asset Manag.*, Vol. 5, No. 3, pp. 261–277, 2015. [10.1108/BEPAM-02-2014-0011](https://doi.org/10.1108/BEPAM-02-2014-0011)
- [11] I. Korolija, Y. Zhang, L. Marjanovic-Halburd, and V. I. Hanby, “Regression models for predicting UK office building energy consumption from heating and cooling demands,” *Energy Build.*, Vol. 59, pp. 214–227, 2013. <https://doi.org/10.1016/j.enbuild.2012.12.005>
- [12] Y. W. Lee, D. M. Strong, B. K. Kahn, and R. W. Wang, “AIMQ: a methodology for information quality assessment,” *Information & Management*, Vol. 40, No. 2, pp.133-146, 2002.
- [13] R. Mikučionienė, V. Martinaitis, and E. Keras, “Evaluation of energy efficiency measures sustainability by decision tree method,” *Energy Build.*, Vol. 76, pp. 64-71, 2014. <https://doi.org/10.1016/j.enbuild.2014.02.048>
- [14] S. Mohandes, A. Abdul Hamid, and H. Sadeghi, “Exploiting building information modeling throughout the whole lifecycle of construction projects,” *J. Basic Appl. Sci. Res.* Vol. 4, No. 9, pp. 16–27, 2014.
- [15] I. Motawa, and A. Almarshad, “A knowledge-based BIM system for building maintenance,” *Automation in Construction*, Vol. 29, pp. 173–182, 2013. <https://doi.org/10.1016/j.autcon.2012.09.008>
- [16] J. Nummelin, K. Sulankivi, M. Kiviniemi, and T. Koppinen, “Managing Building Information and client requirements in construction supply chain — contractor’s view,” in: *Proceedings of the CIB W078-W102 joint conference*, Sophia Antipolis, France, Oct. 2011.
- [17] W. J. O’Brien, R. R. A. Issa, J. Hammer, M. S. Schmalz, J. Geunes, and S. X. Bai, “SEEK: Accomplishing enterprise information integration across heterogeneous sources,” *ITcon* Vol. 7, pp. 101- 124, 2002.
- [18] E. A. Pärn, D. J. Edwards, and M. C. P. Sing, “The building information modelling trajectory in facilities management: A review”. *Automation in Construction*, Vol. 75, pp. 45-55, 2017. <http://dx.doi.org/10.1016/j.autcon.2016.12>
- [19] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A Design Science research methodology for information systems research”, *Journal of Management Information Systems*, Vol. 24, No. 3, pp. 45-77, 2007. <http://dx.doi.org/10.2753/MIS0742-122240302>
- [20] Z. Pourzolfaghar, and M. Helfert, “Investigating HCI Challenges for Designing Smart Environments. In *International Conference on HCI in Business*”, Government and Organizations, pp. 79-90, July 2016. Springer International Publishing.
- [21] Y. Rezgui, A. Zarli and C. J. Hopfe, “Editorial - Building information modeling applications challenges and future directions,” *ITcon* 14, pp. 613-616, 2009.
- [22] W. Shen, Q. Hao, H. Mak, J. Neelamkavil, H. Xie, J. Dickinson, R. Thomas, A. Pardasani, and H. Xue, “Systems integration and collaboration in architecture, engineering, construction, and facilities management: A review”. *Advanced Engineering Informatics*, Vol. 24 No. 2, pp. 196–207, 2010. <https://doi.org/10.1016/j.aei.2009.09.001>
- [23] R. Szewczyk, E. Osterweil, J. Polastre, M. Hamilton, A. Mainwaring, and D. Estrin, “Habitat monitoring with sensor networks,” *Communications of the ACM*, Vol. 47 No. 6, pp. 34-40, 2004. doi: 10.1145/990680.990704
- [24] M. C. Tremblay, A. R. Hevner, and D. J. Berndt, “Focus groups for artifact refinement and evaluation in design research,” In *Communications of the Association for Information Systems* 26, Article 27, Vol 6, No. 1, 2010.
- [25] J. Venable, J. Pries-Heje, and R. Baskerville, A comprehensive framework for evaluation in design science research. In *International Conference on Design Science Research in Information Systems*, 2012, pp. 423-438. Springer Berlin Heidelberg.
- [26] G. M. Winch, *Managing Construction Projects: and information processing approach*. Wiley-Blackwell, 2010.
- [27] Z. Yu, F. Haghghat, B. C. M. Fung, and H. Yoshino, “A decision tree method for building energy demand modeling,” *Energy Build.*, Vol. 42, pp. 1637–1646, 2010. <https://doi.org/10.1016/j.enbuild.2010.04.006>
- [28] The Climate Group, “Enabling the low carbon economy in the information age”, *Smart 2020*, M. Webb, The Climate Group, 2008.
- [29] A. H. Buckman, M. Mayfield, and S. BM Beck, “What is a smart building?” *Smart and Sustainable Built Environment* Vol. 3, No. 2, pp.92-109, 2014. <https://doi.org/10.1108/SASBE-01-2014-0003>

4th Doctoral Symposium on Recent Advances in Information Technology

THE aim of this meeting is to provide a platform for exchange of ideas between early-stage researchers, in Computer Science and Information Systems, PhD students in particular. Furthermore, the symposium will provide all participants an opportunity to get feedback on their studies from experienced members of the IT research community invited to chair all DS-RAIT thematic sessions. Therefore, submission of research proposals with limited preliminary results is strongly encouraged.

Besides receiving specific advice for their contributions all participants will be invited to attend plenary lectures on conducting high-quality research studies, excellence in scientific writing and issues related to intellectual property in IT research. Authors of the two most outstanding submissions will have a possibility to present their papers in a form of short plenary lecture.

TOPICS

- Automatic Control and Robotics
- Bioinformatics
- Cloud, GPU and Parallel Computing
- Cognitive Science
- Computer Networks
- Computational Intelligence
- Cryptography
- Data Mining and Data Visualization
- Database Management Systems
- Expert Systems
- Image Processing and Computer Animation
- Information Theory
- Machine Learning
- Natural Language Processing
- Numerical Analysis
- Operating Systems
- Pattern Recognition
- Scientific Computing
- Software Engineering

SECTION EDITORS

- **Kowalski, Piotr Andrzej**, Systems Research Institute, Polish Academy of Sciences; AGH University of Science and Technology, Poland
- **Lukasik, Szymon**, Systems Research Institute, Polish Academy of Sciences, AGH University of Science and Technology, Poland

REVIEWERS

- **Arabas, Jaroslaw**, Warsaw University of Technology, Poland

- **Atanassov, Krassimir T.**, Bulgarian Academy of Sciences, Bulgaria
- **Balazs, Krisztian**, Budapest University of Technology and Economics, Hungary
- **Bronselaeer, Antoon**, Department of Telecommunications and Information at Ghent University, Belgium
- **Castrillon-Santana, Modesto**, University of Las Palmas de Gran Canaria, Spain
- **Charytanowicz, Malgorzata**, Catholic University of Lublin, Poland
- **Corpetti, Thomas**, University of Rennes, France
- **Courty, Nicolas**, University of Bretagne Sud, France
- **De Tré, Guy**, Faculty of Engineering and Architecture at Ghent University, Belgium
- **Fonseca, José Manuel**, UNINOVA, Portugal
- **Fournier-Viger, Philippe**, University of Moncton, Canada
- **Gil, David**, University of Alicante, Spain
- **Herrera Viedma, Enrique**, University of Granada, Spain
- **Hu, Bao-Gang**, Institute of Automation, Chinese Academy of Sciences, China
- **Koczy, Laszlo**, Szechenyi Istvan University, Hungary
- **Kokosinski, Zbigniew**, Cracow University of Technology, Poland
- **Krawiec, Krzysztof**, Poznan University of Technology, Poland
- **Kulczycki, Piotr**, Systems Research Institute, Polish Academy of Sciences, Poland
- **Kusy, Maciej**, Rzeszow University of Technology, Poland
- **Lilik, Ferenc**, Szechenyi Istvan University, Hungary
- **Lovassy, Rita**, Obuda University, Hungary
- **Malecki, Piotr**, Institute of Nuclear Physics PAN, Poland
- **Mesiar, Radko**, Slovak University of Technology, Slovakia
- **Mora, André Damas**, UNINOVA, Portugal
- **Noguera i Clofent, Carles**, Institute of Information Theory and Automation (UTIA), Academy of Sciences of the Czech Republic, Czech Republic
- **Pamin, Jerzy**, Institute for Computational Civil Engineering, Cracow University of Technology, Poland
- **Petrik, Milan**, Czech University of Life Sciences Prague, Faculty of Engineering, Department of Mathematics, Czech Republic
- **Ribeiro, Rita A.**, UNINOVA, Portugal

- **Sachenko, Anatoly**, Ternopil State Economic University, Ukraine
- **Samotyj, Volodymyr**, Lviv Polytechnic National University, Ukraine
- **Szafran, Bartlomiej**, Faculty of Physics and Applied Computer Science, AGH University of Science and Technology, Poland
- **Tormasi, Alex**, Szechenyi Istvan University, Hungary
- **Wei, Wei**, School of Computer science and engineering, Xi'an University of Technology, China
- **Wysocki, Marian**, Rzeszow University of Technology, Poland
- **Yang, Yujiu**, Tsinghua University, China
- **Zadrozny, Slawomir**, Systems Research Institute, Poland
- **Zajac, Mieczyslaw**, Cracow University of Technology, Poland

Virtual Tour for Smart Home Developed in Unity Engine and Connected with Arduino

Erich Stark, Erik Kučera and Oto Haffner

Faculty of Electrical Engineering and Information Technology
Slovak University of Technology in Bratislava
Bratislava, Slovakia

Email: erich.stark@stuba.sk, erik.kucera@stuba.sk

Abstract—Nowadays, virtual tours are very popular and many people would like to see a virtual house before the acquisition of the real one. The paper demonstrates a creation of a virtual tour for smart home developed in Unity 3D engine. This virtual tour is connected with Arduino microcontroller which has attached several sensors and actuators. These electronic devices react to the events in the virtual tour and vice versa.

I. INTRODUCTION

MODERN forms of visualisation are now realized on the basis of the development of new ICT technologies (e.g. interactive applications made in 3D engine [1], virtual reality or mixed reality). Visualisation of process modelling, identification and control of complex mechatronic systems, elements and drives using virtual and mixed reality allows students to get a much better and quicker understanding of the studied subject compared to conventional teaching methods.

Nowadays, there is a trend of using interactive 3D applications and virtual reality in virtual tours for houses, cars and other products. Also, many interactive 3D applications for education are being developed.

Toyota offers modern virtual showroom [2] for their customers. This showroom was developed using Unreal Engine.

There are also interactive applications from Animech Technologies. This company offers many education modules like Virtual Car, Virtual Truck or Virtual Gearbox [3]. Using these applications students can understand the functioning of mentioned devices and they can look into their interior and detach their individual components in detail.

Very interesting project is a virtual clinic [4]. This project is supported by the University of Miami or Charles R. Drew University of Medicine and Science in Los Angeles. This interactive application offers an insight into the actual functioning of a larger clinic, and they can also try to diagnose patients. Students are thus trained through a real experience with the health system, but this complex system is modelled and simulated in virtual reality.

An absolute novelty is Microsoft HoloLens [5], the arrival of which has led to the emergence of a completely new segment of mixed reality. Mixed reality has unquestionable advantages over virtual reality, as the user perceives a real world and also a virtual world in the same time. The use of this feature is in practice undisputed and it is assumed that mixed reality



Fig. 1. Microsoft HoloLens - mixed reality application (Volvo) [6]

will become a new standard in many areas such as education, marketing, modeling of complex mechatronic systems, etc.

For Microsoft HoloLens there are more education and virtual tour applications.

Application HoloTour [7] provides 360-degree spatial video of historical places like Rome or Peru. The application complements 3D models of important landmarks that have not been retained or supplementary holographic information about elements in the scene.

II. MAIN ASPECTS OF PROPOSED APPLICATION

This paper describes an interactive 3D application that simulates virtual tour of the smart house and its exterior. The application is implemented in Unity engine. As it is the interactive application that responds to the perceptions and changes from the environment, it is necessary to connect it with external hardware which captures the signals from the environment and sends the data to the application. As the best candidate to solve this problem, Arduino family microcontroller has been chosen. Arduino will be connected to the computer via the USB port and connection will be established through the serial port. Through this port, the data from sensors will be sent to the application. It is important to note that communication will not run in only one direction (from Arduino to the computer) but also from the computer to Arduino. So it is possible to control actuators connected to Arduino.

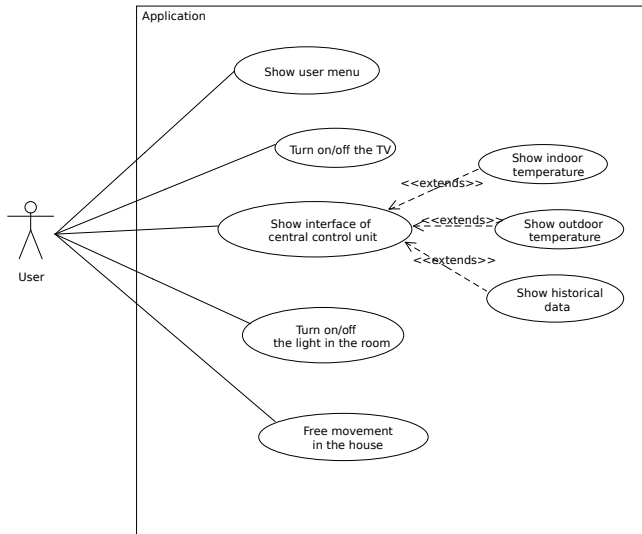


Fig. 2. Use-case diagram

The proposed application has its own data storage. This storage can be used for statistical evaluations or retrieval of historical data. The database was created using cloud service Microsoft Azure [8].

The application must meet these functional requirements:

- option to move in the house and in outdoor areas.
- ability to view the current temperature
- user menu and ability to set COM port for Arduino microcontroller
- ability to turn on/off light in rooms by loud sounds like clapping
- fan rotation on room ceilings when temperature is higher than a certain value
- triggering of fire alarm when detecting the presence of fire in a real environment
- stretching the curtains in the living room in low light conditions and vice versa
- option turn on/off a TV using IR controller when the user is at a sufficient distance from the TV
- option to view historical data about indoor and outdoor temperature
- alerting the user of the unfavourable state of the application

A use-case diagram is in Fig. 2.

III. SENSORS AND ACTUATORS

The application is based on a number of the necessary sensors and actuators connected to the microcontroller:

- fire sensor
- sound sensor
- light sensor
- temperature sensor
- IR receiver

These sensors will be mapped in the application for a certain functionality. Also, few actuators will be used:

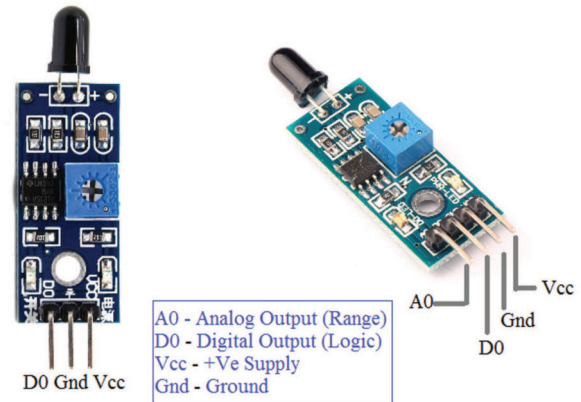


Fig. 3. Fire sensor



Fig. 4. Sound sensor

- LED diode
- buzzer

A. Fire sensor

One of the basic sensors of the proposed system is a fire sensor (Fig. 3) that detects the presence of a flame. In principle, it is a detection of infrared light with a wavelength in the range of 760 to 1100 nm. Its core parts include an infrared sensor, a potentiometer, an operational circuit amplifier and a LED. There are different types of these sensors, but two most well-known are three-pin and four-pin sensors. Four-pin sensors have one pin for the analog connection.

B. Sound sensor

The sound sensor (Fig. 4) is a small board with a microphone that enables sound detecting from the environment. By connecting to the analog pin, it is possible to detect the intensity of the incoming sound.

C. Light sensor

Light sensor (Fig. 5) is also called a photoelectric sensor because it converts light energy into electrical signals. The more light it gets on the surface of the light-sensitive part, the resistance decreases. Normal value ranges from 8 to 20k Ω .



Fig. 5. Light sensor

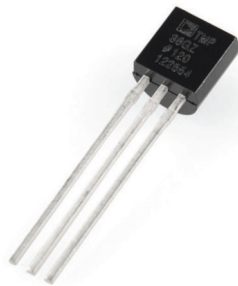


Fig. 6. Temperature sensor

D. Temperature sensor

Temperature sensor (Fig. 6) of type TMP36 is used. It is a low-voltage thermal sensor that provides a voltage output that is proportional to the sensed temperature. This device is also very easy to use and requires no external calibration. The temperature range is from -40°C to $+125^{\circ}\text{C}$ is a very decent result for such a small and simple device, although the accuracy of the measured values may have a deviation of up to 2°C .

E. IR receiver

The last important sensor in proposed project is the infrared receiver (Fig. 7). It has also a built-in infrared transmitter but it is not used. As the infrared transmitter, a modern smartphone can be used.

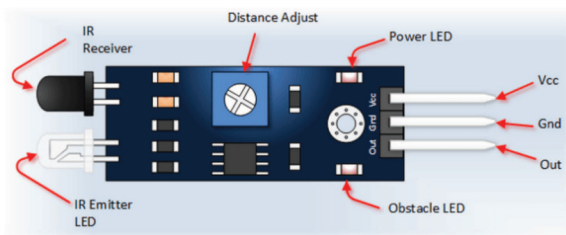


Fig. 7. IR receiver

TABLE I
IDENTIFIERS AND POSSIBLE VALUES FOR SENSORS

Type of sensor	Identifier	Measured value
Light sensor	light	from 0 to 1024
Temperature sensor	temperature	from -40 to 120
Sound sensor	sound	from 0 to 2014
Fire sensor	flame	fire / calm
IR receiver	ir	signal

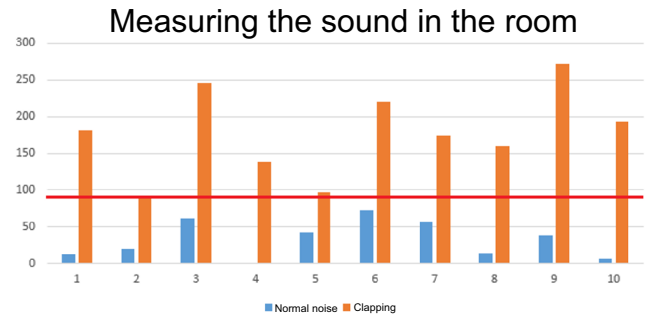


Fig. 8. Measuring the sound in the room

IV. IMPLEMENTATION OF THE APPLICATION

A. Processing data from sensors

As it was mentioned, the data from sensors will come from Arduino in a continuous stream. It is, therefore, important to determine the data format so that we can easily recognize the sensor and what value the sensor has captured. On the Arduino side, an infinitely uninterrupted cycle will take place, and on the Unity side, the C # programming language will provide parsing functions, which will process the information and perform the necessary functionality. The data format is: {sensor}+"_"+"{type_of_sensor}+"_"+"{measured_value}

The first part is a characteristic string that will let us know that there is some data from the sensors. It is important to start with a particular string because if we also have other data from other sources in the application that we would like to send through our application, it might happen that we are simply mixing the data. This is a situation we are, of course, trying to avoid. The second part will be a unique identifier for individual sensors connected to Arduino. The last part will be the measured value we get from the connected sensors. See details in Table I.

A very important part is the definition of boundary values captured on sensors when a system will perform a certain function corresponding to the measured values. One of these values is the volume for the sound sensor which will allow the system to turn on or off the lights in the room. It is important to set this value sufficiently sensitive to clapping near the sensor but at the same time high enough to filter out any ambient noise. Few test has been made (Fig. 8) and it was found that good boundary value would be 90.

Another boundary value in the system is the value of light in the room. If we capture values of light under the certain value

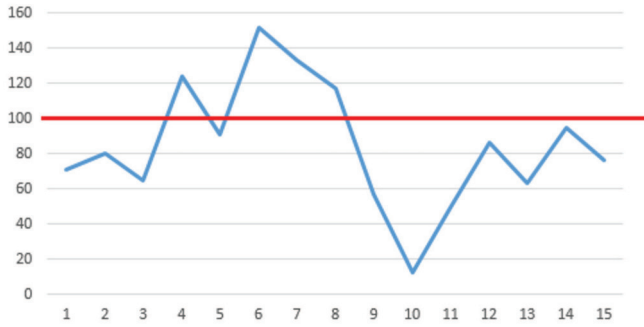


Fig. 9. Measuring the light value

TABLE II
PROPOSED API FOR MYSQL DATABASE

URI	HTTP method	Response data type	Description
uri_of_server/all	GET	JSON	all records
uri_of_server/{id}	GET	JSON	One record with id
uri_of_server/add	POST	boolean	Positive/negative answer according to the success of the operation

(boundary value) the curtains on the ground floor will spread out. To determine the boundary value it was necessary to make several measurements (Fig. 9) in different light conditions. The chosen boundary value is 100.

The last boundary value is the temperature that was set to 27°C.

B. Classes and data

Class diagram can be seen in Fig. 10.

Used MySQL database is closely linked to the API that provides the interface between the database and the application. Our API carries the RESTful service characteristics but we can not fully say that this endpoint meets all REST properties like all CRUD operations but at least it has the proper use of HTTP methods. For our needs, it is not necessary to use all CRUD operations. We have defined three unique URIs through which it is possible to access database data (Table II).

C. Menu and interface

The interface of the application should be simple and understandable. For the proposed application, it is best to use the first person view as it offers the most realistic experience. It is possible to rotate with the mouse and use arrows for basic movement. For future purposes, such control is easy to map in virtual reality. That is why we decided to use a point at the center of the screen instead of a mouse control. Using *Escape* the user turn on/off the main menu (Fig. 11). Another important menu is GUI (12) for temperature inspecting. This menu shows when the user is close to the central control panel in the virtual smart house.

The exterior of the home has been designed to match the overall home visualisation to create the atmosphere of a luxury

smart house with all the equipment from the collection of cars, a swimming pool and trees.

In the interior there are many interactive points that interact with the user in a certain way. These are televisions, lighting, fans, or curtains.

In Fig. 13, there is a living room of the presented smart house. It is possible to see many interactive elements. The first one is a television that can be turned on and off by an external controller. The second one is the curtains that pull and stretch automatically depending on the intensity of the light in the home (i.e. light sensor connected to Arduino) and the third one is the ceiling fans that are spinning at an excessive interior temperature.

Fig. 14 shows the light in the house that can be controlled by clapping. If the user is close to the light and claps, the light turns on or off. For this functionality, the sound sensor is used as it was stated.

On each floor, there is a control unit on the wall (Fig. 15). When the user focuses and clicks on it, the menu (Fig. 12) of the central unit opens.

In Fig. 16 there is the exterior of the smart house.

V. CONCLUSION

Nowadays, there is a trend of using interactive 3D applications and virtual reality in virtual tours for houses, cars and other products. This paper describes an interactive 3D application that simulates virtual tour of the smart house and its exterior. The application is implemented in Unity engine. As it is the interactive application that responds to the perceptions and changes from the environment, it is necessary to connect it with external hardware which captures the signals from the environment and sends the data to the application. In future research, it would be interesting to use this experience and develop the application for mixed reality (e.g. Microsoft HoloLens) that will communicate with real sensors and actuators. In this way, it will be possible to control a real smart house using a mixed reality application.

ACKNOWLEDGMENT

This work has been supported by the Cultural and Educational Grant Agency of the Ministry of Education, Science, Research and Sport of the Slovak Republic, KEGA 030STU-4/2015 and KEGA 030STU-4/2017, by the Scientific Grant Agency of the Ministry of Education, Science, Research and Sport of the Slovak Republic under the grant VEGA 1/0819/17 and by the Tatra banka Foundation within the grant programme Quality of Education, project No. 2016vs046 (Support of education in mechatronics through virtual reality).

REFERENCES

- [1] Triseum. (2017) Variant: Limits. [Online]. Available: <https://triseum.com/calculus/variant/>
- [2] K. Sloan. (2016) Rotor brings toyota showroom 360 to life with unreal engine. [Online]. Available: <https://www.unrealengine.com/showcase/rotor-brings-toyota-showroom-360-to-life-with-unreal-engine>
- [3] A. Technologies. (2014) Virtual gearbox. [Online]. Available: <http://www.animechtechnologies.com/showcase/virtual-gearbox/>

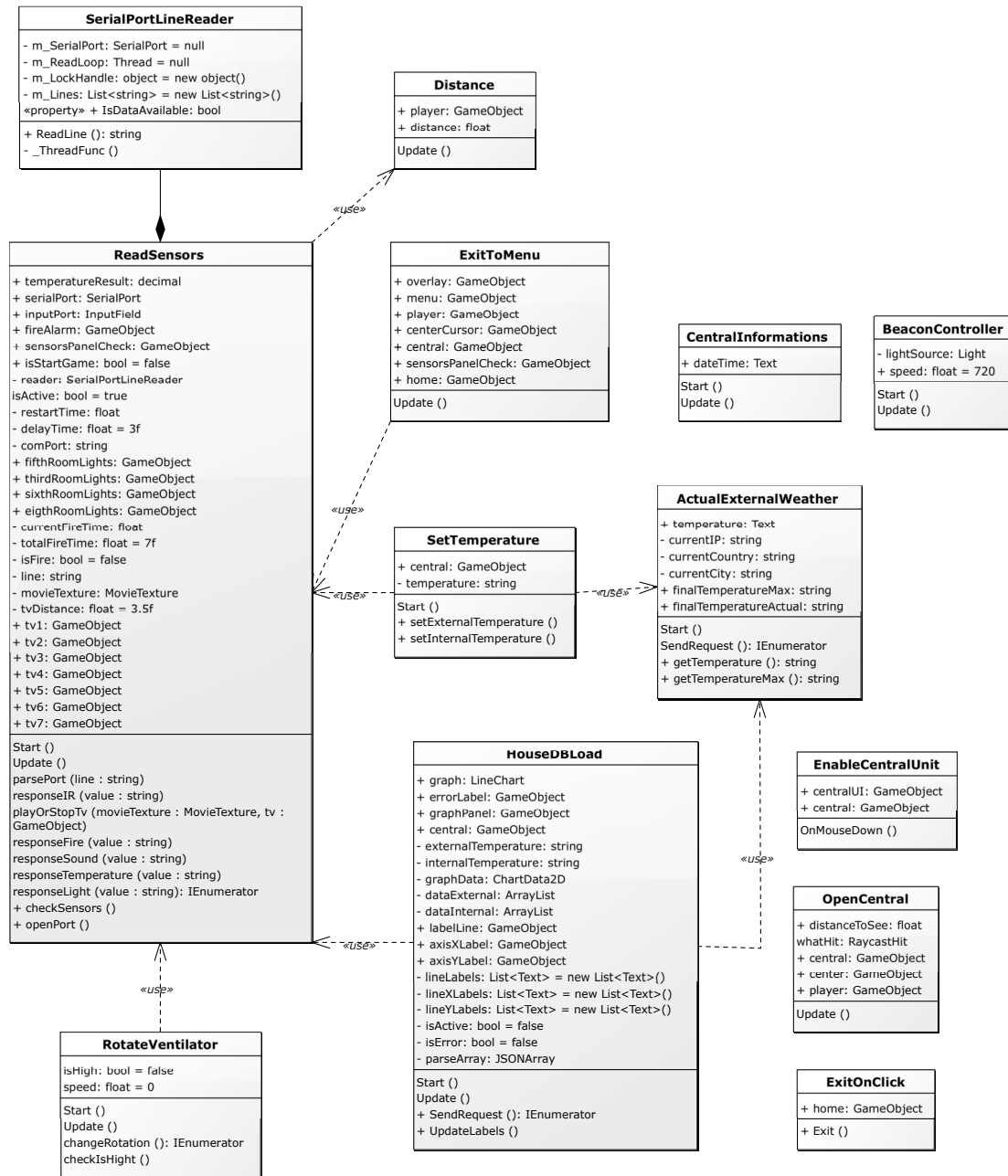


Fig. 10. Class diagram

- [4] D. Parvati, W. L. Heinrichs, and Y. Patricia, "Clinispace: a multiperson 3d online immersive training environment accessible through a browser," *Medicine Meets Virtual Reality 18: NextMed*, vol. 163, p. 173, 2011.
- [5] P. A. Rauschnabel, A. Brem, and Y. Ro, "Augmented reality smart glasses: definition, conceptual insights, and managerial importance," *Working paper, The University of Michigan-Dearborn, Tech. Rep.*, 2015.
- [6] E. Uhlemann, "Connected-vehicles applications are emerging [connected vehicles]," *IEEE Vehicular Technology Magazine*, vol. 11, no. 1, pp. 25–96, 2016.
- [7] M. Corporation. (2017) Holotour. [Online]. Available: <https://www.microsoft.com/en-us/hololens/apps/holotour>
- [8] M. Copeland, J. Soh, A. Puca, M. Manning, and D. Gollob, "Microsoft azure and cloud computing," in *Microsoft Azure*. Springer, 2015, pp. 3–26.

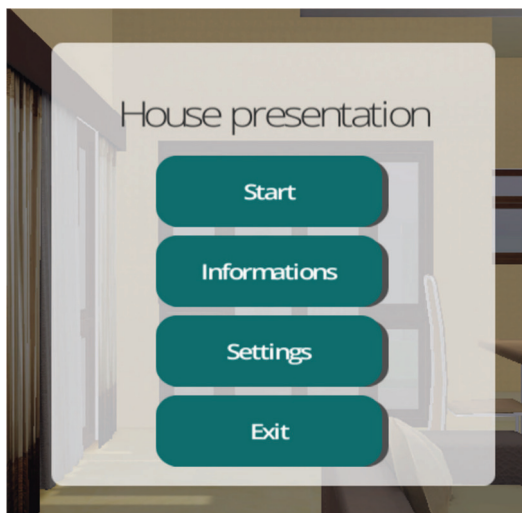


Fig. 11. Main menu



Fig. 14. Lights in the bedroom

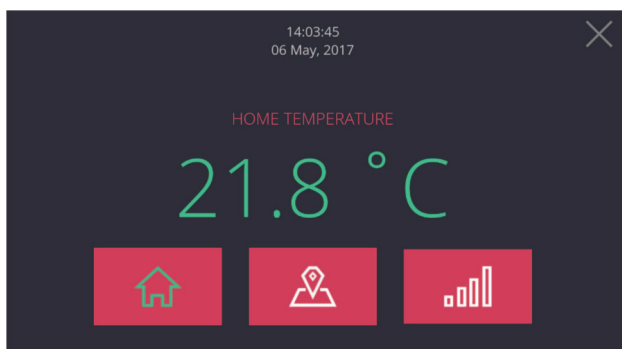


Fig. 12. Temperature menu



Fig. 15. Central control unit



Fig. 13. Interior of the living room



Fig. 16. Exterior

Author Index

- A**
Akpolat, Cem 135
Al-Ali, Rima 187
Albayrak, Sahin 135
Aleti, Aldeida 81
Alirezai, Marjan 71
Ayachi, Faten Labenne 107
- B**
Balcer, Marek 91
Baráth, Áron 97
Bremer, Joerg 61
- C**
Coghetto, Roland 11
Coronato, Antonio 43
- D**
Dąbrowski, Marek 3
- E**
Eklund, Patrik 25
Evina, Pierrette Annie 107
- F**
Fischer, Johannes 51
Fong, Simon 129
- G**
Grabowski, Adam 11
Greenfield, Gary 81
- H**
Haffner, Oto 205
Helfert, Markus 171, 195
- J**
Jaidi, Faouzi 107
Jönsson, Arne 71
- K**
Kamimura, Ryotaro 19
Kučera, Erik 205
- L**
Lehmann, Grzegorz 135
Lehnhoff, Sebastian 61
- M**
Matula, Jiri 153
Michalik, Tomasz 3
Millham, Richard 129
- N**
Nieße, Astrid 61
Nischwitz, Martin 119
Nourani, Cyrus F. 25
Nyström, Mikael 71
- O**
Olszewski, Boguslaw 113
- P**
Pajda, Tomáš 145
Pancerz, Krzysztof 33
Pancham, Jay 129
Paragliola, Giovanni 43
Peters, Daniel 51
Porkoláb, Zoltán 97
Pourzolfaghar, Zohreh 195
- R**
Reinholdtsen, Petter 171
Roka, Rastislav 145
Rot, Artur 113, 177
- S**
Sahinel, Doruk 135
Santini, Marina 71
Seifert, Jean-Pierre 51, 119
Shinkawa, Yoshiyuki 161
Shiraki, Ryoya 161
Sivrikaya, Fikret 135
Sobińska, Małgorzata 177
Sødring, Thomas 171
Stapor, Katarzyna 37
Stark, Erich 205
- T**
Thiel, Florian 51, 119
- W**
Wetzlich, Jan 119
- Z**
Zacek, Jaroslav 153