Security Analysis Models for Multimedia Information Resources in Social Networks

Stanislav Milevskyi[a], Volodymyr Aleksiyev[a], Olha Korol[a], Oleksandr Milov[a], and Serhii Yevseiev[a]

[a] *Simon Kuznets Kharkiv National University of Economics, 9a Nauki ave., Kharkiv, 61166, Ukraine*

Abstract

The paper presents a description of classical and modern multimedia information resources security threats in social networks. It also provides an overview of methods and models for analyzing social networks. Proposed an approach to the creation of a methodology for building security systems for the exchange of multimedia content in social networks through the development of conceptual foundations, methods, and technologies for detecting, assessing, and countering information security threats.

Keywords

Cybersecurity, social networks, multimedia content, security threats.

1. Introduction

The continuous development of global communication services has turned social networks into the dominant segment of information exchange and citizen communication in the virtual space.

The availability of personal media for generating multimedia content and online communities for sharing it has led to explosive growth in the volume of multimedia information that circulates in social networks. In contrast to textual information, for the processing of which there are a wide number of tools and methods [1], for the processing of multimedia content, a wide range of available tools and methods are not observed. Simultaneously with the increase in the volume of multimedia content in social networks, the number, and variety of negative impacts carried out on information resources of a multimedia type or with their help are increasing. Such actions are a source of threats to information security [2].

The growth in the number of users of social networks and multimedia services is currently so active that it outstrips the increase in the world's population. In Fig. 1, it can be seen that the growth rates of the number of users of Facebook and YouTube are significantly higher than the rate of population growth (151.87 and 111.64 compared to 83.873). The increase in information security threats in social networks is directly related to the emergence of such an effect. This can be explained both by an increase in the number and complexity of the content structure and by a significant increase in the number of inexperienced (unprepared, new) users.

Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine

EMAIL: milevskiysv@gmail.com (A.1); aleksiyev@gmail.com (A.2); korol.olha2016@gmail.com (A.3); oleksandr.milov@hneu.net (A.4); serhii.yevseiev@hneu.net (A.5)
ORCID: 0000-0001-5087-7036 (A.1); 0000-0001-6767-7524 (A.2); 0000-0002-7948-5914 (A.3); 0000-0001-6135-2120 (A.4); 0000-0003-1647-6444 (A.5)

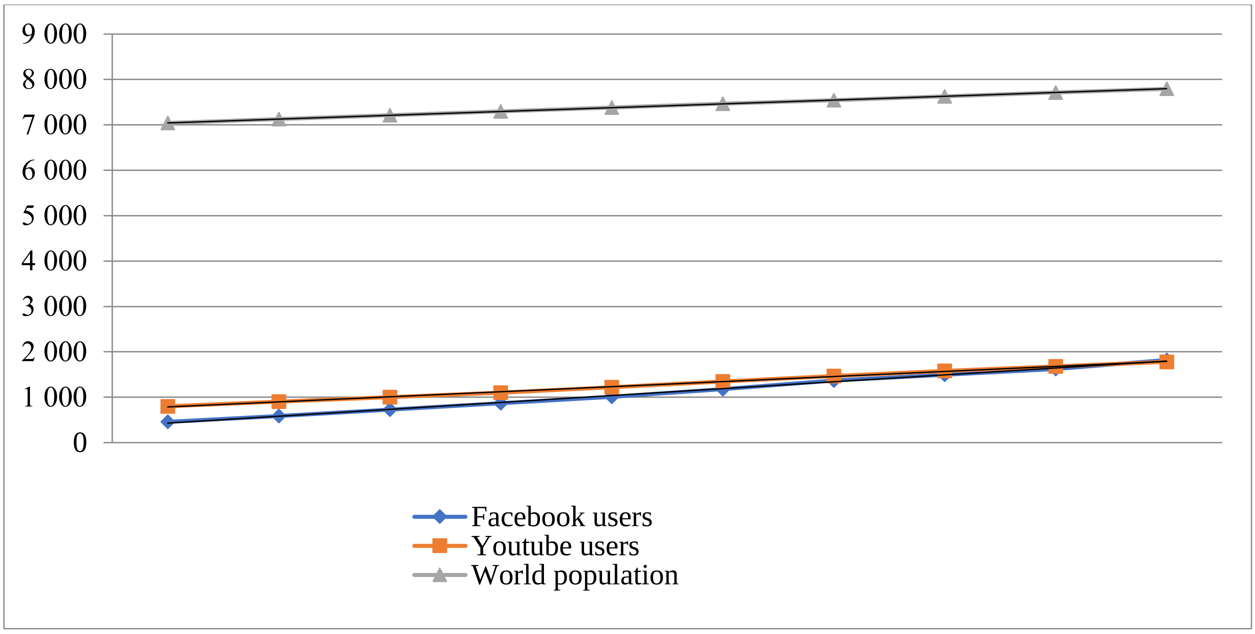

Figure 1: Dynamics of changes in the number of Facebook and Youtube users in comparison with changes in the world's population [3–5]

2. Problem Review

Information security threats are of a different nature and can be implemented using special software or technologies that are inaccessible to the vast majority of users of social networks due to their lack of appropriate professional competence [6] (Fig. 2).

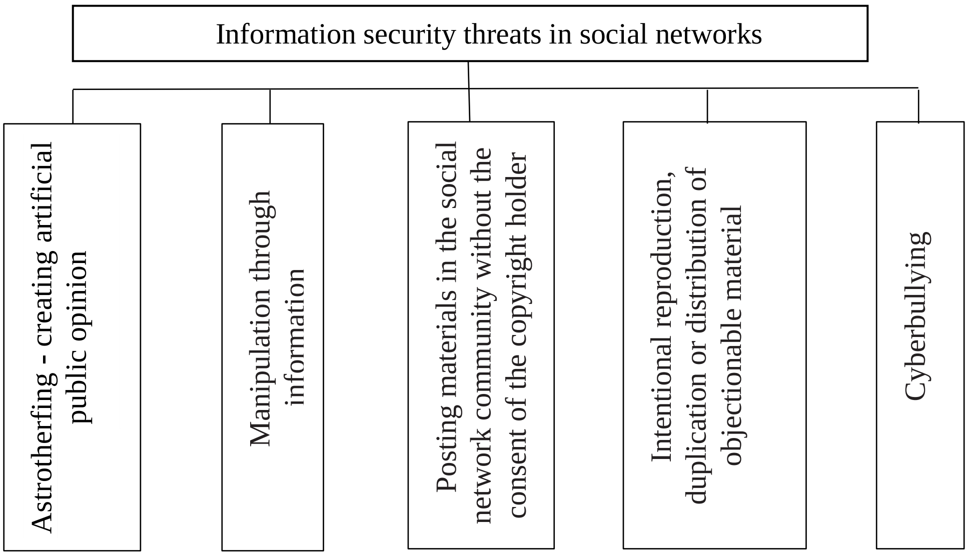
Information security threats in social networks
Astrotherfing - creating artificial public opinion
Manipulation through information
Posting materials in the social network community without the consent of the copyright holder
Intentional reproduction, duplication or distribution of objectionable material
Cyberbullying

Figure 2: Traditional main threats to information security in social networks

Informational and psychological impact on group users by imitating the mass discussion of any information (the so-called astroturfing). This type of threat has a negative impact on the joint work of the group members, reflecting on the consciousness of the participants in the discussion.

Manipulation with information (information overload, misinformation, distortion of information, or mixing true facts with false ones). This threat is capable of affecting the mind and consciousness of the group members, as well as inciting them to carry out destructive and socially dangerous actions.

Posting materials in the social network community without the consent of the copyright holder. The ease of infringement of copyright in community-posted student work leads to unauthorized copying and use of fragments of the work.

Reproduction, duplication, or distribution of objectionable material intentionally posted by group members.

Cyber humiliation and cyberbullying of network members. Humiliation and insult in community discussions destroy the moral and psychological atmosphere and hinders the implementation of activities.

In [7], a specific list of information security threats arising in social networks was highlighted. These threats include spam on social networks, social engineering threats, posting honeypots on social networks, impersonating friends, the possibility of replacing a person or a masquerade, stealing passwords and phishing, using URL shortening services, using the same usernames and passwords in corporate networks and external social resources, web attack, information leakage, and compromise of the behavior of company employees, APT (Advanced Persistent Threat) attack.

3. Research Materials

To effectively reduce the degree of influence of threats to information security in social networks, it is necessary to adequately apply methods of analysis of social networks, which make it possible to identify potential "centers of influence" capable of forming a collective public opinion for destructive purposes.

Currently, in the analysis of social networks, there are four main areas of research [8]: structural, resource, normative and dynamic (Fig. 2).

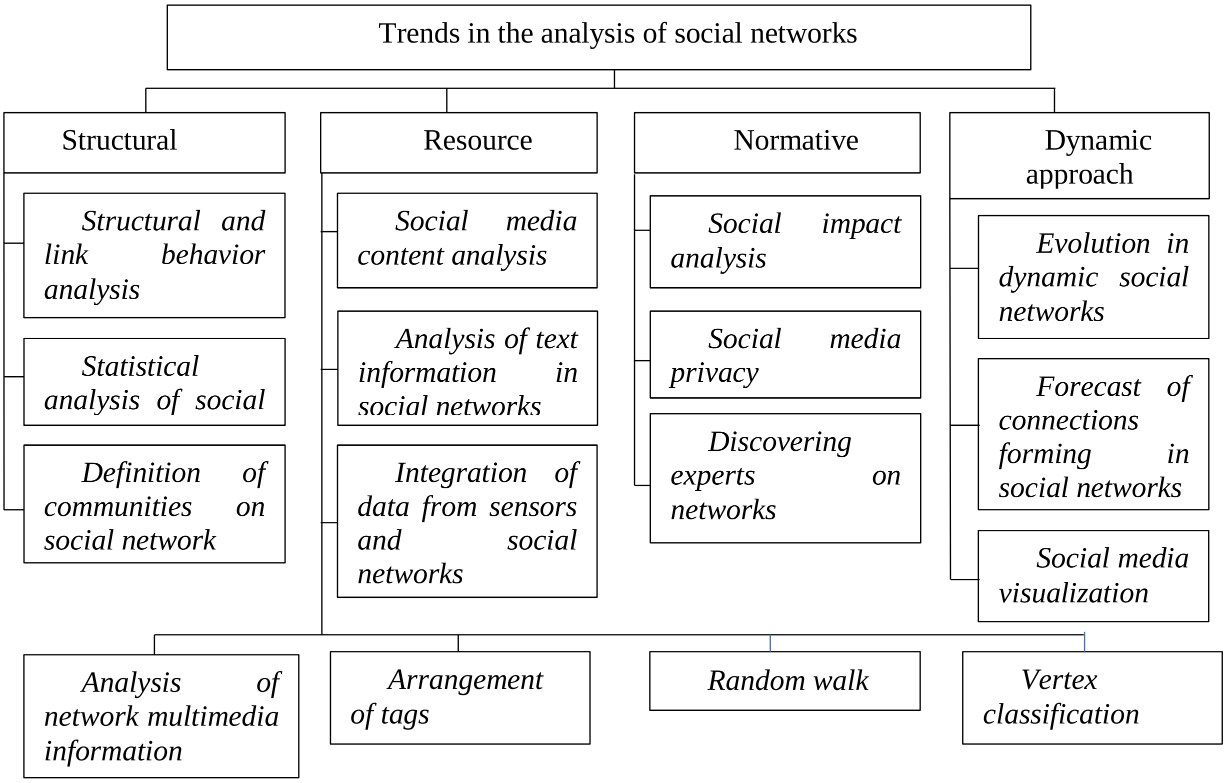
Trends in the analysis of social networks
Structural
Resource
Normative
Dynamic approach
Structural and link behavior analysis
Statistical analysis of social
Definition of communities on social network
Social media content analysis
Analysis of text information in social networks
Integration of data from sensors and social networks
Social impact analysis
Social media privacy
Discovering experts on networks
Evolution in dynamic social networks
Forecast of connections forming in social networks
Social media visualization
Analysis of network multimedia information
Arrangement of tags
Random walk
Vertex classification

Figure 3: Classical approaches to the analysis of social networks

In the structural approach, all network participants are considered as nodes of the graph, which affects the configuration of edges and other network participants. The main attention is paid to the geometric shape of the network and the intensity of interactions (the weight of the edges); therefore, such characteristics as the mutual arrangement of vertices, centrality, and transitivity of interactions are investigated. Structural and network exchange theories are used to interpret the results in this direction.

The resource-based approach considers the possibilities of participants to attract individual and network resources to achieve certain goals and differentiates participants who are in identical structural positions of the social network by their resources. Knowledge, prestige, wealth, race, gender can act as individual resources. Network resources are understood as an influence, status, information, capital.

The normative approach examines the level of trust between participants, as well as the norms, rules, and sanctions that affect the behavior of participants in a social network and the processes of their interactions. In this case, the social roles that are associated with this edge of the network are analyzed, for example, the relationship between the manager and the subordinate, friendship, or family ties. The combination of individual and network resources of a participant with the norms and rules in force in this social network forms his “network capital.” In a simplified form, “network capital” can be viewed as the sum of some advantages that a participant can receive at an arbitrary point in time to achieve a certain goal.

A dynamic approach is a direction in the study of social networks, in which the objects of research are changing in the network structure over time: for what reasons do the edges of the network disappear and appear, how does the network change its structure under external influences, are there any stationary configurations of the social network.

As can be seen from previous, when analyzing social networks, a fairly wide range of problems is solved and methods from various fields of knowledge are applied. However, to directly identify the characteristics and properties of social networks and their segments in order to identify potential sources of threats to information security, it is necessary to consider specific models for analyzing social networks (Table 1).

Table 1.

Social network analysis models *

Model	Content and characteristics of the model
“The power of weak ties” Mark Granovetter	For many social tasks, such as finding a job, weak ties are much more effective than strong ties (ant colony optimization approach)
The small-world phenomenon, or the theory of the six handshakes Milgram	The hypothesis is that each person is familiar with any other inhabitant of the planet through a chain of mutual acquaintances, on average, consisting of six people. So far, this claim has not been refuted. On the contrary, as proof of the correctness of the hypothesis, the observation is put forward that the diameter of most networks is relatively small.
Graph models	Any social network can be mathematically represented as a graph (stochastic block models, probabilistic graph models, conventional graph models)
Analysis of centrality and other local properties	To determine the relative importance (weight) of the graph vertices (that is, how influential a participant is within a particular network), the concept of centrality is introduced—a measure of proximity to the center of the graph.
Algorithm for calculating the level of confidence (TrustRank)	Designed to separate informative web pages from spam. TrustRank is a value that gives an estimate of whether a particular site can be trusted, assuming that it does not contain spam. The more links there are on the site, the less trust is “passed” through each such link. TrustRank decreases with increasing distance between it and the original sample.
Strength of the structural position of the participant	The strength of the structural position is the main indicator that determines the differences in the resources of network participants.
Community detection methods and related subgroup analysis	Community analysis allows studying the stability of social structures. The simplest case of a linked group is a community where each member is associated with everyone, and other members of the network cannot be included in this group, since they do not have

	connections with all members of the community.
Data dimensionality reduction methods	The projection of the network vertices into the Euclidean space of reduced dimension is considered to describe the relationships between the rows and columns of this matrix. As a result, it is possible to visualize changes in the status of a network user against the background of changes in the statuses of subgroups.
Structural equivalence of network participants	The approach is the opposite of exploring related groups. Participants are equivalent when they occupy the same positions in the social structure of the network, that is, when the structure and type of interaction of these participants with others are equivalent, while the equivalent participants in the network should not interact with each other.
Role algebras	The direction of analysis of social networks, which focuses on identifying the logic of interactions of network participants in block models, makes it possible to identify similarities in the principles of relationships between participants in various social networks
Analysis of dyads and triads	Dyads are a set of two network members (vertices) and all interactions (edges) between them. The dyad for each type of interaction can be in one of four states: there is no connection between the participants, the connection is directed from the first participant to the second, the connection is directed from the second participant to the first, mutual connections of the participants. The analysis of dyads helps to establish the probability of the presence of an edge between them, the degree of dependence on the properties of participants, to determine the conditions and directions of information transfer, etc. For triads (three interacting participants), questions of transitivity of interactions are additionally investigated.
Stochastic models	The main idea behind probabilistic directed graph models is that each social network can be viewed as a realization of a random two-dimensional binary array.
Network dynamics models	Consider the strength and speed of changes in connections in social networks (graph evolution models, “closed triangle” model, “forest fires” model)
Algorithmic tools for analyzing the evolution of networks	The algorithms are based on dynamic programming, exhaustive search, maximum matching, and greedy heuristics. The main focus is on identifying approximate user clusters and their temporary changes.
Analysis of network development graphs	Approaches to the analysis of network evolution based on the paradigm of association rule mining and frequent pattern mining. The rules of the evolution of the graph, a new type of frequency models are introduced, and the problem of finding typical models of structural changes in dynamic networks is considered.
Predicting bond formation	Graph evolution models are usually created to evaluate the general statistical properties of existing graphs. You can also try to calculate whether two specific vertices will be connected to each other after a certain period of time. This is a computational task based on the analysis of the evolution of a social network in time and is called the problem of predicting connections.
Ontology-based models	Parameters of social networks can be evaluated using ontologies. First, an analysis of the types of network elements is performed: people, objects (music, photos, videos, messages), interactions

	(knows, reports, comments, etc.). Then the authors use the existing ontology resources and additional options for all kinds of relationships. The FOAF ontology is used to identify the members of a social network and the content they add to the network. A new version of SCOT is used to describe tags.

* Summarized from [8]

Among the many existing models for analyzing social networks, the most interesting are those that can actually be implemented on the basis of available statistical information (metrics of a social network and its participants).

One of these characteristics is the “level of trust.” The algorithm for calculating the level of trust (TrustRank) [9] was created to separate informative web pages from spam. For a control sample, experts manually assess the trust level of a small number of sites that can be considered reliable. These sites are taken as a benchmark. Further, the algorithm is based on the statement that good sites rarely link to bad ones, but bad ones very often link to good ones. TrustRank is a value that gives an estimate of whether a particular site can be trusted, assuming that it does not contain spam. The more links there are on the site, the less trust is “passed” on each such link. TrustRank decreases with increasing distance between it and the original sample.

To strengthen the results of calculating the level of trust, it is advisable to use the indicator “Strength of the structural position of a participant,” which determines the differences in the resources of network participants. In the theory of network exchange, to measure this characteristic, [10] the GPI index of the participant’s strength is introduced v_i (Genuine Progress Indicator):

$$GPI_i = \sum_{k=1}^{g-1} (-1)^{k-1} P[i]_k, \tag{1}$$

where $P[i]_k$ is the number of disjoint paths of length *k*, passing through the vertex v_i. Participant strength v_i compared to the strength of the participant v_j calculated as GPI_{ij} = GPI_i - GPI_j.

It is advisable to track the spread of malicious information from centers of influence using “Network Dynamics Models” [11, 12].

Graph evolution models [13] according to which, when a new vertex is added to the network, vertices are selected to which one can join using the joining preference rule. Also, the selection of a vertex can be performed randomly or by “copying” some of its external links.

Triangle-Closing Model [13] states that new vertices added to the network tend to close the triangle. If we assume that the connections that arise between the participants form a triangle, then an “open” triangle occurs when two participants can be connected with each other only through the third, that is, one of the three connections is missing. When a third bond is added, a “closed” triangle is obtained.

The model of “forest fires” [14] is, in a sense, a generalization of the closed triangle model. The new vertex is joined to the existing one by selecting a subgraph containing this vertex and connecting it to all vertices of this subgraph. The process begins at the selected vertex and resembles the propagation of a fire through all vertices of the network.

In addition, studies [15] have shown that the parameters of social networks (diameter, number of participants, average path length, etc.) can be estimated using ontologies. First, an analysis of the types of network elements is performed: people, objects (music, photos, videos, messages), interactions (knows, reports, comments, etc.). Then the authors used the existing ontology resources and added options for all kinds of connections, including “dad,” “mom,” “friend,” applied the FOAF ontology to determine the participants of the social network and the content that they add to the network. A new version of SCOT was used to describe the tags. An ontology SemSNI (Semantic Social Network Interactions) of interactions in a social network (page visits, comments, private messages) and an ontology for the analysis of social networks SemSNA were created. With the help of these ontologies, within the framework of the semantic analysis of a social network, it was possible to calculate the parameters of the subgraphs of a social network for different types of semantic relations (“family,” “I like” / “favorite,” “friendship” / “isFriendOf”) and types of interactions (“Comments,” “creates a message,” etc.).

4. Results Discussion

However, to build an effective security system for multimedia content in social networks, it is necessary to develop an algorithm based on the use of available information about participants, groups, and communities. This will allow developing a mechanism for identifying threats and identifying the sources of their occurrence.

To develop a methodology for constructing security systems for multimedia information resources in social networks, the concept of modeling the behavior of members of a social network is proposed, which is implemented at three levels.

At the first level, an element of a social network (agent or actor) is determined, the behavior of which forms the behavior of the social network as a whole, and is decisive for the study and construction of a security system. At this level:

1. A set of actions of an individual element of a social network is determined, which together form behavior.
2. The probabilities of the implementation of certain actions are determined.
3. Information multimedia resources associated with a particular action are determined.
4. Possible attacks aimed at the corresponding information resources are determined.
5. Cost indicators of the corresponding information resources are determined.

At the second level, models of collective behavior (group dynamics) are built. At this level:

1. Models of influence in the group are determined.
2. The dynamic characteristics of the group's behavior are determined—stability, coordination of actions, self-organization of the group, temporal characteristics of the dynamics of behavior.
3. Characteristics of openness, isolation, or closedness of the group are determined.

At the third level, threats are identified that are directed at the platform of the functioning of the social network as a whole. At this level, a classifier of threats specific to social networks and their multimedia content is formed (or modified).

The formed complex of tasks, separated by levels, makes it possible to form an economically grounded methodology for constructing a security system for multimedia information resources of social networks.

The methodology construction process consists of five stages:

1. Analysis of a social network and possible attacks on it.
2. Analysis of a social network and possible attacks on it.
3. Development of models of the social network group level.
4. Development of platform-level models for the functioning of a social network.
5. Development of methods for determining the most likely threats and assessment of their cost indicators.

The inclusion of economic indicators in the model for analyzing the security of multimedia information resources in social networks will expand the capabilities of detecting threats and sectors of influence (critical nodes) in social networks.

5. Conclusion

The use of standard models of analysis of social networks at the present stage does not allow identifying the sources of threats to the security of multimedia information resources in social networks. This is primarily due to the fact that the main tool of influence is multimedia content, which, unlike text content, is not subject to indexing to increase search speed. Mass identification of multimedia content in modern conditions is possible only on the basis of the name of the file itself and hashtags on the corresponding page. This problem critically affects the development of effective models for analyzing multimedia information resources in social networks and requires the development of a new methodology for identifying and countering information security threats.

6. References

[1] K. V. Molodetska-Grinchuk, Influence of information in the social Internet services on the basis of intellectual analysis of text content, in: Proceedings of the 3rd Intern. scien.-practical. conf. Up-to-date food security for cyber security and information security, Kiev, 2017, pp. 120–121.

[2] R. V. Grishchuk, K. V. Molodetska-Grinchuk, Statement of the problem of securing the information security of the state in social Internet services, Modern defense of information 3 (2017) 86–96.

[3] Facebook: number of daily active users worldwide 2011-2020. URL: https://www.statista.com/statistics/346167/facebook-global-dau/

[4] Global number of YouTube viewers 2016-2021. URL: https://www.statista.com/statistics/805656/number-youtube-viewers-worldwide/

[5] UN Department of Economic and Social Affairs Population Dynamics. URL: https://population.un.org/wpp/Download/Standard/Population/

[6] I. D. Rudinskiy (Ed.), N. A. Davydova, S.V. Petrov, Competence. Expertise. Competence approach, Hotline – Telecom, Moscow, 2018.

[7] L. Kirichenko, T. Radivilova, O. Baranovskyi, Detecting cyber threats through social network analysis, International Journal “Information Technologies & Knowledge” 11 (2017) 23–48.

[8] T. Batura, Methods of analysis of computer social networks, Bulletin of Novosibirsk State University, Series: Information Technology, 01/01 vol. 10 (2012) 13–28.

[9] Z. Gyöngyi, H. Garcia-Molina, J. Pedersen, Combating Web Spam with TrustRank, in: Proceedings of the International Conference on Very Large Data Bases, 2004, pp. 576.

[10] M. Davern, Social Networks and Economic Sociology: A Proposed Research Agenda for a More Complete Social Science, American Journal of Economics & Sociology56 (1997) 287–302.

[11] F. Bonchi, C. Castillo, A. Gionis, A. Jaimes, Social Network Analysis and Mining for Business Applications, ACM TIST 2 (2011) 22–58.

[12] R. Hanneman, Computer-Assisted Theory Building: Modeling Dynamic Social Systems. Riverside, CA,University of California, Riverside, 1988.

[13] J. Leskovec, J. Kleinberg, C. Faloutsos, Graphs over Time: Densification Laws, Shrinking Diameters and Possible Explanations, in: Proceedings of the 11th ACM SIGKDD International Conference on Knowledge Discovery in Data Mining (KDD), N. Y., 2005, pp. 177–187.

[14] J. Leskovec, L. Backstrom, R. Kumar, A. Tomkins, Microscopic Evolution of Social Networks, in: Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, N. Y., 2008, pp. 462–470.

[15] G. Érétéo, F. Gandon, M. Buffa, O. Corby, Semantic Social Network Analysis, in: Proceedings of the 8th International Semantic Web Conference, 2009, pp. 180–195.