A Reputation Mechanism to Support Cooperation of IoT Devices*,**

Giancarlo Fortino[1], Lidia Fotia[2], Fabrizio Messina[3], Domenico Rosaci[4], and Giuseppe M. L. Sarné[2]

[1] DIMES, University of Calabria, Via P. Bucci, cubo 41c, 87036 Rende (CS), Italy
giancarlo.fortino@unical.it
[2] DICEAM, University "Mediterranea" of Reggio Calabria, Loc. Feo di Vito, 89122 Reggio Calabria, Italy {lidia.fotia,sarne}@unirc.it
[3] DMI, University of Catania, Viale Andrea Doria 6, 95126 Catania
messina@dmi.unict.it, italy
[4] DIIES, University "Mediterranea" of Reggio Calabria, Loc. Feo di Vito, 89122 Reggio Calabria, Italy domenico.rosaci@unirc.it

Abstract. A critical issue for small and low-cost Internet of Things (IoT) devices facing multiple complex, advanced and interactive tasks trying to save their power resources. To reach these goals IoT devices can use the capabilities of nearby devices having suitable resources, given that they make their resources available for free or with a determined cost. In such a context, IoT devices can take significant benefits by exploiting the social attitude of software agents to mutually interact and cooperate with other agents they consider as trustworthy. However, in wide communities it is common that a lot of members are unreferenced with respect to the own trustworthiness and, therefore, the task of carrying out a reliable choice about a potential partner can be very difficult. To tackle such an issue, we propose an agent framework where each IoT device is associated with an agent that helps its device in choosing reliable partners for its tasks. To this aim, we designed a reputation model implementing some countermeasures against malicious IoT devices. To verify the efficiency and effectiveness of our proposal, we carried out some experiments in a simulated scenario, which confirmed the potential advantages deriving by its adoption.

Keywords: IoT · Reputation · Software Agent

1 Introduction

The Internet of Things (IoT) [3, 20] age is characterized by environments formed by "smart" objects able to cooperate among them and with users to make use-

** The authors contributed equally to this work that has been developed at the Networks and Complex Systems (NeCS) Laboratory - Department of Engineering Civil, Energy, Environment and Materials (DICEAM) - University Mediterranea of Reggio Calabria.

ful and attractive services [6, 7, 19]. Such smart environments are pervasively populated by small and low-cost IoT devices that, in turn, have the problem of balancing performance and power autonomy [32].

To this aim, a large number of researches have been addressed to optimize these aspects also by increasing the level of engagement of IoT devices with the rest of the world. Consequently, innovative solutions capable to optimize hardware/software resources also by saving power have been proposed. In this respect, for instance, several cloud-based environments have been developed for allowing the access to perform communication, computational and storage resources [17], also managed by different physical and/or virtual components living on the cloud.

In the IoT scenario, an interesting challenge is to promote the mutual cooperation among IoT devices by making available unused resources belonging to nearby and more equipped and performing devices, for free or for pay[5]. In the past, a similar approach was used to improve temporarily the service level of an Internet provider by sharing the unused Wi-Fi bands of its residential clients [1] or proposed to offer Internet connections cheaper than those of traditional providers [11].

In such sharing contexts, a basic and shared requirement is a strong attitude to trust strangers but the choice of inappropriate counterparts can expose to several potential threats for malicious, fraudulent and/or disliked behaviors [37]. The threat is very common in open and heterogeneous environments and/or in presence of economic mechanisms like payments. To deal with this issue, we argue the necessity of a certain level of confidence and mutual trustworthiness for motivating sharing actors to interact on the basis of a reasonable hope to be engaged in profitable interactions with reliable partners. To this aim, trust and reputation systems can improve the mutual confidence between counterparts and mitigate risks due to the presence of unreliable partners [16]. In particular, trust and reputation systems provide some measures about the expectations of a trustor to receive some type of benefit from a trustee. These measures are obtained on the basis of direct or indirect information about past behaviors or events [14],

In this paper we deal with an IoT scenario where a wide community of mobile IoT devices can exploit the opportunity to mutually cooperate, in order to exploit resources hold by some peers. The underlying idea of our proposal is of exploiting an agent-based architecture and a reputation system. In particular, to tackle the management of cooperative tasks is proposed an agent-based framework where: *i*) each IoT device hosts a software tamper-proof agent (i.e., device agent) managing reputation information in a safe manner [10, 18] as well as capable of basic interactions and social behaviors with other agents; *ii*) a number of different kind of agents are distributed into the IoT environment to offer some basic services to all the agents associated with the IoT devices; *iii*) a distributed

[5] Note that authentication, cooperation protocol and payment issues are considered as orthogonal with respect to the focus of our proposal and, therefore, they are not dealt in the following of this paper.

reputation-system is deployed in the environment to support device agents when deleting a partner to perform their daily tasks.

We observe that the adoption of tamper-prof device agents eliminates the need to adopt any centralized component, since every device agent maintains its own reputation measure by itself and spreads it only when interacts (in a safe manner [27]) with other device agents [28]. However, in requiring/accepting cooperation, notice that if an agent has an adequate knowledge of its potential partner, deriving by its experiences (i.e., reliability), it could decide also of not exploiting the reputation information.

The plan of the paper is as follows. Section 2 gives an overview on the related literature. Section 3 introduces the proposed agent framework, while Section 4 describes the adopted reputation model. The experimental results are presented in Section 5 and in Section 6 some conclusions are drawn.

2 Related Work

In open, competitive and distributed scenarios, an important issue is represented by realizing a comfortable environment where the involved actors can perform their own activities. In this respect, it is necessary to limit the large number of possible, potential threats and vulnerabilities typical of such environments [37].

To this aim, trust and reputation systems are able to mitigate threats and vulnerabilities risks and supporting the choices of reliable partners to cooperate [9, 16, 21]. Given its interdisciplinary nature, trustworthiness issues has been widely investigated and a large number of analysis, models and architectures intersecting many scientific areas can be found in the literature. The interested reader might refer to a considerable number of surveys that investigated on the state-of-the-art in this field, among which [29, 33, 38, 42].

From a practical point of view, trust affects almost every decision process and social interaction involving both human and virtual activities [5, 25, 44]. The most relevant factors affecting the computation of trust and reputation measures inside a community are *i*) the nature and the quality of the informative sources [26], *ii*) the rules for aggregating trustworthiness information [13] and *iii*) the modalities for inferring trust into the community (e.g., by adopting a a centralized or a distributed approach) [30]. In particular, some studies found that the accuracy of a local trust approach, based on the own ego-network [12], is greater with respect to a global approach in presence of an adequate number of information, which tightly depends on the adopted horizon depth [45] that, in turn, affects the computation costs.

However, in large communities both *i*) the computation of a global trust can be complex (or also infeasible) and *ii*) each member usually interacted only with a narrowest share of its community (and, therefore, the most part of the community members is unknown and unreferenced). As a consequence, in such scenarios, local trust is particularly predominant and some studies verified that the most accurate results are obtained in inferring trust values on the shorter paths (i.e., those paths closer to the trustor) [23].

A convenient way, to represent trust processes happening in a community is that of using a graph, *trust network*, where members are associated with nodes and trust relationships (usually sparse) are associated with oriented links. Topological properties of the trust networks have been used by a significant number of proposals like, for instance, in [22] where a variant of the Breadth First Search is adopted to gather the reputation scores and, by using a voting, to compute an updated reputation rate for each user, while in [24] trust scores are propagated only by using fixed length paths. Note that trust and voting processes, even though different from a practical viewpoint are conceptually similar. Indeed, both a trust measure and a vote represent an expectation on one or more future events placed on someone or something and both well fit with the presence of communities denoted by a great population and poor communication opportunities or, like some IoT devices, by hardware and software constraints.

Finally, we introduce some proposals of trust systems conceived for IoT. Currently, researchers are paying attention to the features of these environments by proposing specific techniques [39–41]. For example, in [4] two interacting IoT devices trust each other device and spread evaluations to the other nodes with a *word of mouth* approach. In [34], the authors propose a model that uses reliability and local reputation measures; in particular, each node assesses the trustworthiness of its friend nodes and the opinions of the common friends. In [8], a trust system analyzes the dynamic evolution of social relationships and implements a trust-based service management that adapts to the trust fluctuations. Also, the authors, in [31], suppose that the IoT devices identities are previously unknown and calculate the trust between two devices based on past interactions.

3 The Agent Framework

In this section we describe the Agent Framework (AF), which is illustrated in Figure 1. Let us denote by $\mathbf{C}$, $\mathbf{D}$ and $\mathbf{A}$, respectively the IoT environment, the set of all IoT devices and the set of their associated device agents. For sake of simplicity, the set of agents and their relationships will be represented by using a graph $G = \langle N, L \rangle$, where N represents the set of nodes belonging to G and each node $n \in N$ is associated with a unique agent $a \in A$, while L is the set of oriented links where each link $l \in L$ represents a relationship occurring between two agents.

The proposed scenario includes mobile IoT devices requiring cooperation, denoted by r, to other IoT devices, denoted by p, that can accept, for free or for pay, or refuse to share their resources. We denote the generic device by $d_k \in \mathbf{D}$ with $k = \{r, p\}$ specifying his/her role of cooperation requester or provider.

The AF includes two type of agents, respectively named: *i*) *Device agent*, denoted by $a^{d_k} \in \mathbf{A}$; *ii*) *Framework agent*, denoted by $F \in \mathbf{C}$. The first type of agents live on the IoT devices, while the other type of agents are distributed on the AF to provide some basic services to the other agents. Note that all the agents in AF are provided with a shared pair of asymmetrical cryptographic keys.

A main aim of the framework agents (i.e., F), which are safe agents that have their identity certified by a Certification Authority, is to register device agents on the AF the first time they came active on AF and giving them an initial reputation ρ (see below). Instead, the aim of a device agent is that of managing reputation information, included the reputation score of its IoT device, and to select the best potential partner for cooperation by exchanging information about counterparts identities and reputations (obtained by interacting with the other device agents active in its neighbor).

Device agents perform three coordinated activities, denoted as *Search*, *Choice* and *Updating*. More in detail:

- *Search*. In particular, when an IoT device d_r, active in a specific area, is searching for a cooperation task t_r (e.g., for a service) then its device agent a^{d_r}:
  - spreads a signed message m_r consisting of a tupla $m_r = \langle d_{id}, t_r, \rho_r \rangle$, where d_{id} is the identification code of d_r, t_r is the required task, ρ_r is the reputation of d_r;

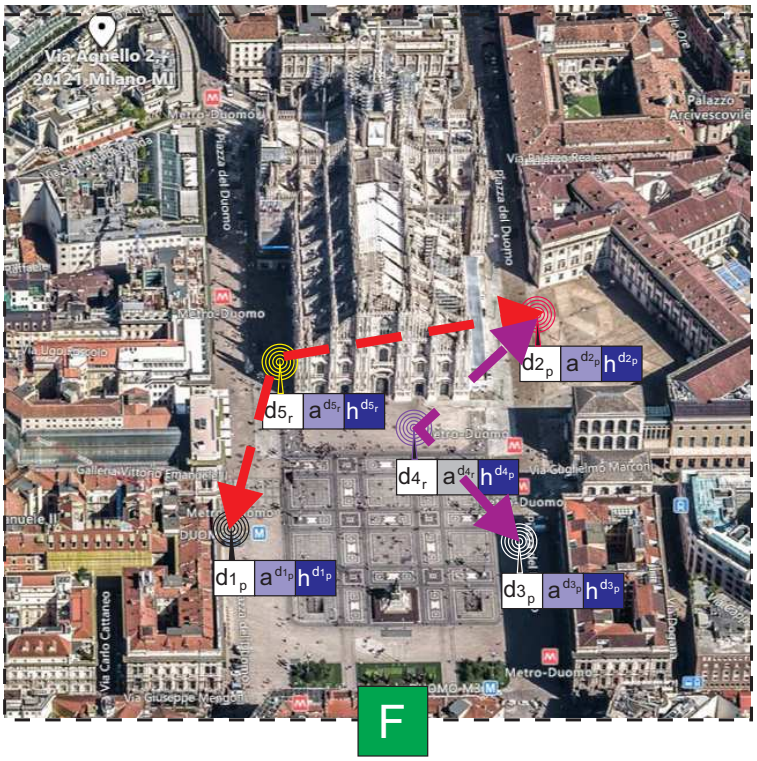

Fig. 1. The AF scenario where IoT devices $d1_p$, $d2_p$ and $d3_p$ can provide cooperation to IoT devices $d4_r$ and $d5_r$ that require it.

  - collects and analyzes all the answers received from each nearby IoT device (i.e., d_p) that has the willing of cooperating for t_r with d_r also based on the d_p reputation score by taking into account the d_r individual *hazard threshold* $[15, 35]$ which represents the probability of "failure" that the requester considers as acceptable. Such answer messages have the form of $m_p = \langle d_{id}, t_r, \rho_p, c \rangle$ where the first three terms have the same meaning specified above and the last element c is the cost required for cooperation (c is set to 0 if the cooperation is provided for free).
- *Choice*. Based on both the required cooperation costs and its hazard threshold (see above) chooses the best possible partner to cooperate with respect to the received proposals. When a partner choice is taken then the two devices start to cooperate. Remember as authentication, cooperation protocol and payment issues are not considered because beyond the focus of this paper.
- *Updating* If a cooperation have had place then the two devices, by means of their agents, provide to exchange in a safe manner their feedback and update their reputation scores (see below).

4 The Reputation Model

The proposed reputation model provides each IoT device with a reputation score, computed on the basis of observations about past behaviors, and represents a synthetic esteem about expected future behaviors of that IoT device [2]. In particular, at the end of each cooperation between two device, the counterpart realeases a feedback. Therefore, based on the received feedback the reputation score of each involved IoT device is updated to enclose its behavior history.

Let be d_i and d_j two generic cooperating IoT devices and let be $\phi^r_{j,i} \in [0, 1] \subset \mathbb{R}$ the feedback released by d_i about the quality of the cooperation for the task t_r provided by d_j, where 0 means the minimum appreciation and, conversely, 1 means the maximum appreciation for the cooperation. In order to limit some malicious and collusive behaviors, the released feedback $\phi^r_{j,i}$ is weighted by some parameters taking into account the competence and honesty of d_j in providing a reliable feedback (i.e., γ_j), the cooperation cost for the task t_r (i.e., $\mu^r_{j,i}$) and number of interaction already occurred in the past between d_i and d_j (i.e., $\varepsilon_{j,i}$). More in detail:

- the parameter γ_j takes into account how many, in average, the feedback released by d_j are closed to the reputation scores of the target devices, more formally:

$$\gamma_j = \begin{cases} 1 & \text{if } \dfrac{\sum_{i=1, i \neq j}^{n} (\phi^r_{j,i} - \rho_i}{n} \leq \chi \\ 0 & \text{Otherwise} \end{cases} \qquad \forall i \in \text{AF} \text{ and } \chi \in [0, 1] \subset \mathbb{R} \tag{1}$$

  where χ is a system parameter (see Section 5);
- $\mu^r_{j,i}$ takes into account of the real or virtual value of the cooperation cost c^r for the task t_r and its value is: *i*) proportional to the ratio c^r / C_{Max} otherwise. *ii*) set to 1 if the cost is greater than a cost threshold C_{Max} (see Section 5).

This approach hinders malicious behavior aimed to earn reputation for free or low cost cooperation tasks to cheat in case of expansive cooperation tasks.

$$\mu_{j,i}^{r} = \begin{cases} 1 & \text{if } c \geq C_{Max} \\ c^{r}/C_{Max} & \text{if } 0 < c^{r} < C_{Max} \end{cases} \tag{2}$$

– $\varepsilon_{j,i}$ is aimed to mitigate collusive IoT devices activities addressed to mutually increasing their reputation scores by exchanging, with high frequency, positive feedback (i.e., $\phi_{j,i}^{r} \geq 0.5$) and depends on how many times d_j provided a feedback to d_i with respect to a given threshold W of consecutive cooperation tasks. More formally, $\varepsilon_{j,i}$ is computed as:

$$\varepsilon_{j,i} = \begin{cases} 1 & \text{if } \phi_{j,i}^{r} < 0.5 \\ 1/\lambda_{j,i} & \text{if } \phi_{j,i}^{r} \geq 0.5 \end{cases} \tag{3}$$

where, with respect to a feedback given by d_j about d_i, the value of $\lambda_{j,i}$ is: *i*) set to 1 the first time that a feedback is released; *ii*) increased by 1 every time that a new feedback is released before that other W cooperation tasks have been carried out; *iii*) computed as the maximum between 1 and $\left(\lambda_{j,i} - \left\lfloor \frac{\Delta w}{W} \right\rfloor\right)$ when the distance Δw, in terms of cooperation tasks, between two consecutive feedback is greater or equal than W.

Finally, the reputation score of the IoT device d_i will be updated for the feedback $\phi_{j,i}^{r}$ released by d_j only if *i*) $\rho_i \geq 0.5$ and *ii*) $\gamma_j \cdot \left(\frac{\mu_{j,i}+\varepsilon_{j,i}}{2}\right) \cdot \phi_{j,i}^{r} > 0$ as follows:

$$\rho_i{}^{new} = \alpha \cdot \rho_i{}^{old} + (1-\alpha) \cdot \gamma_j \cdot \left(\frac{\mu_{j,i} + \varepsilon_{j,i}}{2}\right) \cdot \phi_{j,i}^{r} \tag{4}$$

where the parameter α influences the behavior of the reputation system (see Section 5), since the higher is its value, the lower is the sensitivity of ρ.

Given the peculiarity of the IoT scenario, the solution adopted to store and spread reputation scores is that of providing the device agents of tamper-proof capabilities and, like other software applications, they can ensure the reliability of the information spread in their AF activities. In such a way, device agents can be considered also as local stubs of the Framework agents.

Furthermore, to contrast whitewashing strategies and some malicious behaviors a number of countermeasures are in place. For instance, *i*) to hinder whitewashing strategies [43] without penalizing new members [36], the initial reputation assigned to each IoT device is set to 0.5, while *ii*) possible malicious behaviors aimed to avoid receiving negative feedback by realizing a communication fail, are detected by the IoT device which monitors the device activities, and are penalized by decreasing the reputation score of the IoT device as $\rho_i{}^{new} = \sigma \cdot \rho_i{}^{old}$, where the system parameter $\sigma \in [0, 1[\subset \mathbb{R}$ is determined proportionally to the ratio of communication faults involved in the IoT device life.

5 Experiments

To verify the effectiveness of the proposed reputation model, a campaign of simulations have been realized in a large IoT scenario. In particular, 10,000 IoT devices requiring cooperation and 500 IoT devices providing cooperation to them have been simulated. Simulations have been organized for epochs and each of them has been formed by 50 epochs, a number of epochs suitable to obtain stable and significant trends, and for each epoch only 2500 IoT devices (i.e., the 25% of the overall population), randomly chosen, were active to search for cooperation.

In particular, two different scenarios have been simulated and their descriptions and parameter settings are summarized in Table 1. The first scenario (A) presents *i*) a number of malicious actors providing unreliable feedback to their counterparts, like 0 instead of 1 or vice versa, and *ii*) a probability π of communication failure. The second scenario (B) presents malicious and collusive actors aimed to access and cheat on expensive cooperation tasks by increasing their reputation on the basis of cooperation tasks having a low cost or provided for free (i.e., alternate behavior). To this purpose, the ratio between low and high costs for cooperation tasks was assumed to be $1:4$.

To identify IoT devices reliable in providing feedback, the parameter χ has been set to 0.5 (see Eq.1), such that agents having a unreliable behavior have a probability τ to receive feedback less than 0.5 (see Table 1). Moreover, at the beginning of each simulation, the initial reputation (i.e., ρ) of each IoT device was set to 0.5.

Scenario	Malicious IoT devices	Malicious Behavior
A	10%	Malicious devices gives incorrect feedback and interrupt communication with probability π
B	10%	Malicious IoT devices build a positive reputation thanks to low cost/free cooperation tasks for cheating on high cost cooperation tasks. Any interruption of communication occurs.
$\alpha = 0.5$,	$W = 5$,	$\rho = 0.5$, $\chi = 0.5$ $\pi = 0.5$, $\tau = 0.8$

Table 1. The simulated scenarios and system parameters

To measure the performance of the proposed reputation system acting in an IoT scenario, we considered *i*) the percentage of malicious IoT devices that, sooner or later, assume values of reputation reflecting their behavioral nature with respect the overall IoT device population, named in the following *Malicious Percentage* (MP) and *ii*) the average value of reputation of the malicious IoT device, named *Average Malicious Reputation* (AMR).

Figures 2 and 3 graphically represent the obtained results for the MP and AMR measures with respect to the simulated scenarios A and B, respectively. More in detail, Figure 2 highlights as the proposed reputation model works

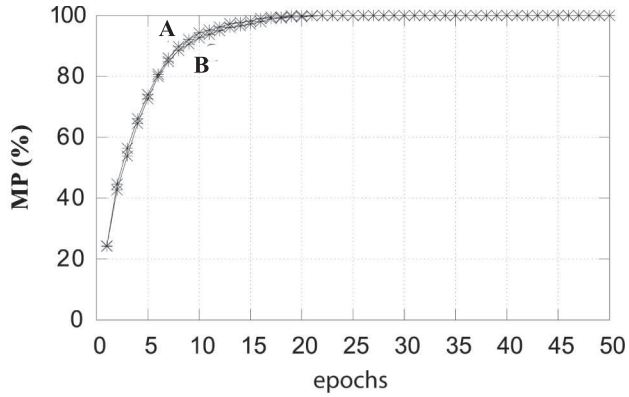

Fig. 2. Malicious Percentage (MP) measures (only distrusted IoT device) for 50 epochs of simulations. Scenarios A and B.

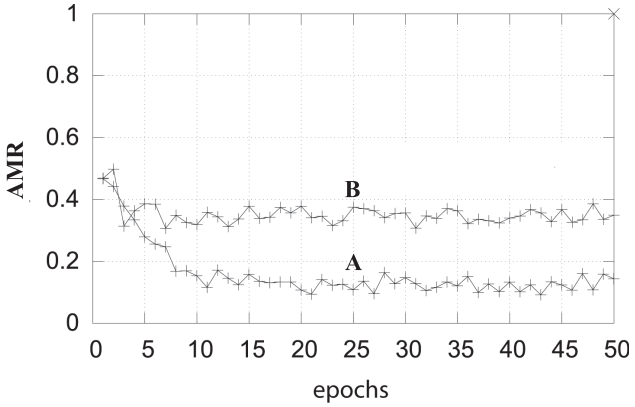

Fig. 3. Average Malicious Reputation (AMR) measures (only distrusted IoT devices) for 50 epochs of simulations. Scenarios A and B.

well in identifying unreliable IoT devices, indeed for both the scenarios the MP measures quickly assumes a value greater than 90% after about 10 epochs (i.e., when the number of transactions carried out becomes significant) with irrelevant differences occurring between the scenarios A and B (affected by alternate behaviors). Figure 3 shows as for the scenario A the AMR curve quickly reaches values lower than 0.2, while the trend of the AMR measure for the scenario B is rather different due to the alternate behavior but, however, the AMR measure assumes values around 0.37 that is lower than 0.5 which is the threshold differentiating honest by dishonest IoT devices.

The presented preliminary results have shown as the proposed reputation system is effective and able to quickly identifying all the "malicious" IoT devices without "false positive" in the proposed scenarios.

6 Conclusions

In this paper, we proposed an agent-based distributed approach to support cooperation among IoT devices in order to save their resources. In particular, each IoT device is associated with a software agent to easily interact and cooperate among them. In such a context, the possibility of leading satisfactory interactions is tightly connected to the selection of a reliable counterpart. As we explained, when no suitable information are available to perform a good choice, it is necessary to ask information about potential partners to those agents considered as mostly trustworthy. To this aim, the reputation model we proposed it is capable to minimize the impact due to malicious collusive activities carried out by dishonest IoT devices. To validate our approach we performed a set of simulation of the described agent framework. The results proved the effectiveness of our reputation model in identifying malicious and collusive actors as well as to hinder their bad actions.

As future work, we are planning to study the reputation model also with respect to different combination of related parameters.

References

1. Vodafone wi-fi community. available at URL: http://www.vodafone.it/portal/privati/vantaggi- vodafone/per-i-gia-clienti/wifi-community
2. Abdul-Rahman, A., Hailes, S.: Supporting trust in virtual communities. In: HICSS '00: Proc. of the 33rd Hawaii Int. Conf. on System Sciences. vol. 6. IEEE Computer Society. (2000)
3. Ashton, K.: That' internet of things' thing. rfid journal, 22 june 2009 (2009)
4. Bao, F., Chen, I.R.: Dynamic trust management for internet of things applications. In: Proceedings of the 2012 international workshop on Self-aware internet of things. pp. 1–6. ACM (2012)
5. Buccafurri, F., Fotia, L., Lax, G.: Social signature: Signing by tweeting. In: International Conference on Electronic Government and the Information Systems Perspective. pp. 1–14. Springer (2014)
6. Casadei, R., Fortino, G., Pianini, D., Russo, W., Savaglio, C., Viroli, M.: A development approach for collective opportunistic edge-of-things services. Information Sciences **498**, 154–169 (2019)
7. Casadei, R., Fortino, G., Pianini, D., Russo, W., Savaglio, C., Viroli, M.: Modelling and simulation of opportunistic iot services with aggregate computing. Future Generation Computer Systems **91**, 252–262 (2019)
8. Chen, R., Bao, F., Guo, J.: Trust-based service management for social internet of things systems. IEEE transactions on dependable and secure computing **13**(6), 684–696 (2016)
9. Comi, A., Fotia, L., Messina, F., Pappalardo, G., Rosaci, D., Sarné, G.M.L.: Forming homogeneous classes for e-learning in a social network scenario. In: IDC IX, pp. 131–141. Springer (2016)
10. Comi, A., Fotia, L., Messina, F., Pappalardo, G., Rosaci, D., Sarné, G.M.L.: Using semantic negotiation for ontology enrichment in e-learning multi-agent systems. In: 2015 Ninth International Conference on Complex, Intelligent, and Software Intensive Systems. pp. 474–479. IEEE (2015)

11. Comi, A., Fotia, L., Messina, F., Pappalardo, G., Rosaci, D., Sarné, G.M.L.: A distributed reputation-based framework to support communication resources sharing. In: Intelligent Distributed Computing IX, pp. 211–221. Springer (2016)
12. De Meo, P., Fotia, L., Messina, F., Rosaci, D., M. L. Sarné, G.M.L.: Providing recommendations in social networks by integrating local and global reputation. Information Systems **78**, 58–67 (2018)
13. Dellarocas, C.: Designing reputation systems for the social web. SSRN Electronic Journal (2010)
14. Dumouchel, P.: Trust as an action. European J. of Sociology/Archives Européennes de Sociologie **46**(3), 417–428 (2005)
15. Falcone, R., Castelfranchi, C.: Social Trust: a Cognitive Approach. Kluwer Academic Publishers, Norwell, MA, USA. (2001)
16. Fogel, J., Nehmad, E.: Internet social network communities: Risk taking, trust, and privacy concerns. Computers in Human Behavior **25**(1), 153–160 (2009)
17. Fortino, G., Messina, F., Rosaci, D., Sarné, G.M.L.: Using trust and local reputation for group formation in the cloud of things. Future Generation Computer Systems **89**, 804–815 (2018)
18. Fortino, G., Gravina, R., Russo, W., Savaglio, C.: Modeling and simulating internet-of-things systems: A hybrid agent-oriented approach. Computing in Science & Engineering **19**(5), 68–76 (2017)
19. Fortino, G., Russo, W., Savaglio, C., Shen, W., Zhou, M.: Agent-oriented cooperative smart objects: From iot system design to implementation. IEEE Transactions on Systems, Man, and Cybernetics: Systems (2017)
20. Fortino, G., Trunfio, P.: Internet of things based on smart objects: Technology, middleware and applications. Springer (2014)
21. Fotia, L., Messina, F., Rosaci, D., M. L. Sarné, G.M.L.: Using local trust for forming cohesive social structures in virtual communities. The Computer Journal **60**(11), 1717–1727 (2017)
22. Golbeck, J., Hendler, J.: Inferring binary trust relationships in web-based social networks. ACM Transactions on Internet Technology **6**(4), 497–529 (2006)
23. Golbeck, J.: Computing and applying trust in web-based social networks. In: PhD Thesis. University of Maryland, Department of Computer Science (2005)
24. Guha, R., Kumar, R., Raghavan, P., Tomkins, A.: Propagation of trust and distrust. In: Proc. of the 13th International Conference on World Wide Web. pp. 403–412. ACM (2004)
25. Heidemann, J., Klier, M., Probst, F.: Online social networks: A survey of a global phenomenon. Computer Networks **56**(18), 3866–3878 (2012)
26. Huynh, T., Jennings, N., Shadbolt, N.: An integrated trust and reputation model for open multi-agent systems. Autonomous Agents and Multi-Agent Systems **13**(2), 119–154 (2006)
27. Jansen, W.A.: Countermeasures for mobile agent security. Computer Communications **23**(17), 1667–1676 (2000)
28. Josang, A., Gray, E., Kinateder, M.: Simplification and Analysis of Transitive Trust Networks. Web Intelli. and Agent Sys. **4**(2), 139–161 (2006)
29. Jøsang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decision support systems **43**(2), 618–644 (2007)
30. Kim, Y., Song, H.: Strategies for predicting local trust based on trust propagation in social networks. Knowledge-Based Systems **24**(8), 1360–1371 (2011)
31. Mahalle, P.N., Thakre, P.A., Prasad, N.R., Prasad, R.: A fuzzy approach to trust based access control in internet of things. In: Wireless Communications, Vehicular

Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 2013 3rd International Conference on. pp. 1–5. IEEE (2013)
32. Mahmoud, M.S., Mohamad, A.A.: A study of efficient power consumption wireless communication techniques/modules for internet of things (iot) applications. Advances in Internet of Things **6**(02), 19 (2016)
33. Momani, M., Challa, S.: Survey of trust models in different network domains. arXiv preprint arXiv:1010.0168 (2010)
34. Nitti, M., Girau, R., Atzori, L., Iera, A., Morabito, G.: A subjective model for trustworthiness evaluation in the social internet of things. In: Personal Indoor and Mobile Radio Communications (PIMRC), 2012 IEEE 23rd International Symposium on. pp. 18–23. IEEE (2012)
35. Perich, F., Undercoffer, J., Kagal, L., Joshi, A., Finin, T., Yesha, Y.: In Reputation We Believe: Query Processing in Mobile Ad-hoc Networks. In: Proc. of the First Annual International Conf. on Mobile and Ubiquitous Systems: Networking and Services, 2004 (MOBIQUITOUS 2004). pp. 326–334. Maryland Univ., Baltimore, MD, USA. (aug 2004)
36. Ramchurn, S., Huynh, D., Jennings, N.: Trust in multi-agent systems. Knowledge Engeenering Review **19**(1), 1–25 (2004)
37. Roman, R., Zhou, J., Lopez, J.: On the features and challenges of security and privacy in distributed internet of things. Computer Networks **57**(10), 2266–2279 (2013)
38. Sherchan, W., Nepal, S., Paris, C.: A survey of trust in social networks. ACM Computing Surveys (CSUR) **45**(4), 47 (2013)
39. Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in internet of things: The road ahead. Computer networks **76**, 146–164 (2015)
40. Stergiou, C., Psannis, K.E., Kim, B.G., Gupta, B.: Secure integration of iot and cloud computing. Future Generation Computer Systems **78**, 964–975 (2018)
41. Takabi, H., Joshi, J.B., Ahn, G.J.: Security and privacy challenges in cloud computing environments. IEEE Security & Privacy **8**(6), 24–31 (2010)
42. Vamsi, P.R., Kant, K.: Systematic design of trust management systems for wireless sensor networks: A review. In: Advanced Computing & Communication Technologies (ACCT), 2014 Fourth International Conference on. pp. 208–215. IEEE (2014)
43. Zacharia, G., Maes, P.: Trust management through reputation mechanisms. Applied Artificial Intelligence. **14**(9), 881–907 (2000)
44. Zhan, J., Fang, X.: Social computing: the state of the art. International Journal of Social Computing and Cyber-Physical Systems **1**(1), 1–12 (2011)
45. Ziegler, C., Lausen, G.: Spreading activation models for trust propagation. In: e-Technology, e-Commerce and e-Service, 2004. EEE'04. 2004 IEEE International Conference on. pp. 83–97. IEEE (2004)