This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.

Trustworthiness Management in the Social Internet of Things

Michele Nitti, Roberto Girau, Luigi Atzori, *Senior Member, IEEE* Department of Electrical and Electronic Engineering - University of Cagliari, 09123 Cagliari, Italy
{*michele.nitti, roberto.girau, l.atzori*}*@diee.unica.it*

***Abstract*—The integration of social networking concepts into the Internet of Things has led to the Social Internet of Things paradigm, according to which objects are capable of establishing social relationships in an autonomous way with respect to their owners with the benefits of improving the network scalability in information/service discovery.**

Within this scenario, we focus on the problem of understanding how the information provided by members of the social IoT has to be processed so as to build a reliable system on the basis of the behavior of the objects. We define two models for trustworthiness management starting from the solutions proposed for P2P and social networks. In the subjective model each node computes the trustworthiness of its friends on the basis of its own experience and on the opinion of the friends in common with the potential service providers. In the objective model, the information about each node is distributed and stored making use of a Distributed Hash Table structure so that any node can make use of the same information. Simulations show how the proposed models can effectively isolate almost any malicious nodes in the network at the expenses of an increase in the network traffic for feedback exchange.

***Index Terms*—Internet of Things, social networks, trustworthiness management**

I. Introduction

The Internet of the Future (IoF) is expected to be dominated by huge content-oriented traffic, intensive interactions between billions of persons often on the move, heterogeneous communications among hosts and smart objects, and provisioning of millions of (new) services, with strict real-time requirements and striking flexibility in connecting everyone and everything. Key component of the IoF is then the Internet of Service (IoS), which is aimed at making every possible service (from the management of the own house pantry to the management of the whole company production process) widely and easily available through the Internet yielding to higher productivity. Strictly linked to the IoS is the Internet of Things (IoT), which is aimed at embodying into the Internet a large number of objects that through standard communication protocols and unique addressing schemes provide services to the final users. IoT is then somehow a part of the IoS when the information provided by the objects are seen as services, which are specifically aimed at making information about the physical world available on the Internet [1].

A big value of the IoF resides on its ability to create powerful network of resources, i.e. in making resources social. Such social relationships would great facilitate the discovery of resources that have the capabilities required to solve a particular task. To achieve this goal the IoF should be endowed with the ability to define, build, manage, and access social relationships between resources. Whereas this is currently a reality for the relationships among humans through the technologies for the social Web, still great efforts are needed for an effective management of the social relationships for the other types of resources with only high-level solutions appeared on the literature.

In the IoT world, there are interesting papers that proposed the introduction of social relationships among objects. For instance, in [2] the authors introduce the idea of objects able to participate in conversations that were previously only available to humans. Analogously, the research activities reported in [3] consider that, being things involved into the network together with people, social networks can be built based on the Internet of Things and are meaningful to investigate the relations and evolution of objects in IoT. This has also brought to the convergence of IoT and social network paradigms, as analyzed in [4], which depicts the scenarios where an individual can share the services offered by her smart objects with her friends or their things through widespread social networks. In [5] and [6], explicitly, the Social IoT (SIoT) concept is formalized, which is intended as a social network where every node is an object capable of establishing social relationships with other things in an autonomous way according to rules set by the owner. This new paradigm is also stimulated by the concept that the many are smarter than the few [7], so that objects should interact intensely to converge to opinions and information supported by the crowd.

Until now, in these proposals the focus has been directed to the definition of the relationships and interactions among objects and to the definition of reference architectures and protocols. But the paradigm still lacks in some basics aspects such as understanding how the information provided by the other members have to be processed so as to build a reliable system on the basis of the behavior of the objects. Indeed, without effective trust management foundations, attacks and malfunctions in the IoT will outweigh any of its benefits [8].

On the basis of these observations, the purpose of this work is to address this uncertainty and to suggest strategies to establish trustworthiness among nodes. The challenge is of building a reputation-based trust mechanism for the IoT that can deal effectively with certain types of malicious behavior that intend to mislead other nodes. The major contributions of the paper are the followings:

- Definition of the problem of trustworthiness management

Digital Object Indentifier 10.1109/TKDE.2013.105

in the social IoT, where the objects autonomously establish social relationships and use the resulting network to find the trusted peer(s) that can provided the desired service when needed.
- Definition of two models for trustworthiness management starting from the solutions proposed for P2P and social networks. In the subjective model, more similar to the social scenario, each node computes the trustworthiness of its friends on the basis of its own experience and on the opinion of the friends in common with the potential service provider. In the objective model, obtained starting from the P2P scenario, the information about each node is distributed and stored making use of a DHT (Distributed Hash Table) structure so that any node can make use of the same information.
- Evaluation of the benefits of the trustworthiness management in the IoT, which shows how it can effectively isolate almost any malicious nodes in the network at the expenses of an increase in the network traffic caused by the exchange of feedback information.

In Section II we present the scenario of the social IoT and provide a survey of the research on trustworthiness management in P2P and social networks. In Section III we define the problem and introduce the used notations, whereas in Section IV we illustrate the two models proposed. Section V presents the system performance and Section VI draws final remarks.

II. Background

In the first subsection we summarize the main features of the Social IoT we refer to. In the second subsection we review the techniques that have been proposed for trustworthiness management in P2P networks. This scenario is similar to ours, as in both cases there are services or objects that provide and request information from other peers and then in both cases the evaluation of the reliability of the members of the community is vital. However, it is not beneficial to apply directly, as they are, the solutions seen for P2P systems to the Social IoT, since all the information about the social aspects would be lost. Indeed, works dealing with trust evaluation in human social networks, which we review in the third subsection, provide us with important contributions on how to exploit the concepts of centrality, credibility and link characteristics in trust evaluation in the Social IoT.

A. The Social Internet of Things

The idea to use social networking elements in the Internet of Things to allow objects to autonomously establish social relationships is gaining popularity in the last years. The driving motivation is that a social-oriented approach is expect to put forward the discovery, selection and composition of services and information provided by distributed objects and networks that have access to the physical world [2], [5], [6] and [9].

In this paper, without losing of generality, we refer to the social IoT model proposed in [10] (we use the acronym SIoT to refer to it). According to this model, a set of forms of socialization among objects are foreseen. The *parental object relationship* is defined among similar objects, built in the same period by the same manufacturer (the role of family is played by the production batch). Moreover, objects can establish *co-location object relationship* and *co-work object relationship*, like humans do when they share personal (e.g., cohabitation) or public (e.g., work) experiences. A further type of relationship is defined for objects owned by the same user (mobile phones, game consoles, etc.) that is named *ownership object relationship*. The last relationship is established when objects come into contact, sporadically or continuously, for reasons purely related to relations among their owners (e.g., devices/sensors belonging to friends); it is named *social object relationship*. These relationships are created and updated on the basis of the objects features (such as: object type, computational power, mobility capabilities, brand) and activity (frequency in meeting the other objects, mainly).

To manage the resulting network and relationships, the foreseen SIoT architecture is made of four major components among others [6] and [10]. The *Relationship management* introduces into the SIoT the intelligence that allows objects to start, update, and terminate relationships. *Service discovery* is finalized to find which objects can provide the required service in the same way humans seek for friendships and information. *Service composition* enables the interaction among objects. *Trustworthiness management* is aimed at understanding how the information provided by other members has to be processed. Indeed, this is the core issue of this paper that will be extensively addressed in the following.

B. State of the Art in P2P Networks Trust Management

There are only few works about the trust management in IoT. In [11], the authors propose a model based on fuzzy reputation for trust evaluation to enforce things cooperation in a WSN of IoT/CPS based on their behaviors. In [12], by the use of social trust and QoS trust, a hierarchical trust management protocol is proposed. In [13], the authors use a service classification estimation table to evaluate the user's trustworthiness. In [14] users' trustworthiness in social networks is used to assist the service composition between objects.

Instead, problem of interacting with unknown peers and isolating malicious peers has been deeply investigated in P2P networks. To calculate a peer trustworthiness, a system has to store the reputation information, encourage the sharing of this information among the peers, and define the rules that from the reputation bring to the peer trust level (see Table I).

There are different approaches that can be used to store trustworthiness information. As described in [15], all information can be stored in a centralized storage to foster sharing and make easy the processing; however, it easily leads to a single point of failure. In [16] , the information is distributed in storage peers. Other approaches are the rater-based storage [17], where each peer stores trustworthiness information about the peers it has observed, and the ratee-based storage [18], where each peer stores its own reputation information recorded during the past transactions.

For a reputation system is important to incentive the peers to cooperate and solve some well-known problems, such as

TABLE I
APPROACHES USED FOR THE STORAGE, SHARING, AND PROCESSING OF THE REPUTATION INFORMATION

Storage	Sharing	Processing
Centralized	Local	Average
Distributed	Part	Weighted Average
Rater-Based	Global	Probabilistic Estimation
Ratee-Based		

Free-riders [19] and Tragedy of Commons [20]. A solution is the one proposed in [21], where a peer can buy and sell reputation information from/to other peers and loses credit if it behaves maliciously. When a peer decides to share its information, the system has to cope with how effectively share them. This problem can be handled in different ways: local share, part share, and global share. In local share, each peer manages only the information it is involved with [22]. In part share, each peer shares the information with a set of specific peers. In [17], the authors propose to share the data through a reputation chain of acquaintances and neighbors, since it is more reliable than using random peers [17] [18], and in [23] peers have the possibility to periodically exchange their information. In global share, a mechanism is adopted to collect the information of all peers. This can be done both with a centralized storage [15] and with a distributed storage [16] .

Once the information is collected, it is important to use a computation system that is able to extract a reliable value of the trustworthiness. A simple mechanism relies on the use of an arithmetic average [24] of all the reputation values a node has received. Other models apply a weight to the reputation values in different ways: in [25], the authors use different weights for acquaintance and stranger peers; in [26] the weights are chosen on the basis of the last reputation value a node has received; [27] considers the similarities between two peers in terms of released feedback to weight the reputation value. In [16] , the authors assume the existence of a digraph of social links between peers, where reputation values are assigned to the link based on the transactions between the peers connected through a link. Finally, some algorithms make use of probabilistic estimation techniques [28], [29]. and the maximum likelihood estimation [29] to match the reputation value into the probability that a peer will cooperate.

C. State of the Art in Social Networks Trust Management

In the past few years, online social networks have become more and more popular and consequently several methods to calculate trust, and sometimes distrust between two person [30] have been proposed, together with key applications to allow users to secure their data [31]. In these scenarios, it is considered a person (say Alice) to trust another person (say Bob) if her actions are based on the belief that Bob's behavior will lead to a good outcome. However, some works (e.g., [32]), add another dimension to the traditional probability model of belief and disbelief, considering ignorance as an essential part of human behavior.

In [33], the authors classify online social networks in three generations based on the level of sociality they present and present trust relation mechanisms for each generation. The first generation is characterized by weak sociality where the relationship between partecipants is implicit and the partecipants can not make a new friend with a friend's friend; the second generation has medium sociality and relationship between partecipants is only binary (friend or not friend), but partecipants have the possibility to extend their relationship list by adding friends of friends even if only inside the same social network platform. In the third generation of social network, different types of relationship exist and partecipants can establish new relationships and conduct activities across different social networks. Furthermore, multiple types of relationship between users have lead to the development of relationship-based techniques for trust management in Social Networks [34] [35]. According to this definition, it is possible to consider the SIoT belonging to the third generation with explicit non binary relationship between participants.

The main properties of trust are well defined and many works contribute to describe them ([36], [37], [38], [39] and [40]). One of the most important and controversial is the *transitivity*, based on the concept of recommendation of someone that is not directly known, i.e., if Alice trusts Bob and Bob trusts Eric then Alice trusts Eric. Indeed, it has been demonstrated in [40] that in real life trust is not always transitive but depends on the particular service requested. In [39], constraints are given so that trust can be considered transitive if the trust edges have the same purpose and only in this case the trust system can exploit this property. These constraints imply that different trust matrixes have to be stored for every service, since if Alice trusts Bob for fixing her car, she could not trust Bob for advising her a good restaurant.

Another important property is called *composability*. It is the ability to compose the recommendations from different friends into a unique value and then decide whether to trust or not someone. With different trust values from different friends, a composition function is needed in order to obtain accurate results.

Since trust is related to a person's past experience, another important property in social network is the *personalization*. Accordingly, it's not unusual that two people have different opinions about the same person. For the same reason, trust is also *asymmetric*, i.e., two people tied by a relationship may have different levels of trustworthiness each other.

III. INTRODUCTION TO THE PROPOSED SOLUTION

The SIoT provides the objects with some capabilities of the humans when looking for and providing information in their social communities, i.e., the objects mimic the human social behavior [6]. The type of relationships that have been devised for the SIoT have been taken from some sociology and anthropology studies (e.g., [41] and [42]). [10] provides some experimental analyses when implementing this behavioral model on the IoT. As in most of the IoT architectures, in SIoT the owner has the control on the object functions and social interactions. Among the supervision functionalities, the system (the object) asks the owner to authorize the provisioning of a particular service/piece of information to other objects'

requests. The owner then empowers the object to allows for providing the service or not depending on the specific request (requesting object owner identity and interaction context). This is done at the first occurrences whereas the system learn and behave accordingly for the next transactions. The owner behavior indeed depends on the (direct and indirect) relationships with the requester and on his personality (collaborative, selfish, greedy, malicious and other).

Within this scenario, we aim at designing and experimenting a dynamic trust model for assessing the trustworthiness level of nodes. The next subsection describes the used notation, the second subsection illustrates the trust models, and the third one described the main elements used in the adopted models.

A. Notation and Problem Definition

The main focus of this paper is the design of a dynamic trust model for assessing the trustworthiness level of nodes in a Social Internet of Things. In our modelling, the set of nodes in the SIoT is $\mathcal{P} = \{p_1, ..., p_i, ...p_M\}$ with cardinality M, where p_i represents a generic node. In our problem setting, let the network be described by an undirected graph $\mathcal{G} = \{\mathcal{P}, \mathcal{E}\}$, where $\mathcal{E} \subseteq \{\mathcal{P} \times \mathcal{P}\}$ is the set of edges, each representing a social relation between a couple of nodes. Let $\mathcal{N}_i = \{p_j \in \mathcal{P} : p_i, p_j \in \mathcal{E}\}$ be the neighbourhoods of node p_i, namely the nodes that share a relation with p_i, and $\mathcal{K}_{ij} = \{p_k \in \mathcal{P} : p_k \in \mathcal{N}_i \cap \mathcal{N}_j\}$ be the set of common friends between p_i and p_j.

Let $\mathcal{S}_j$ be the set of services that can be provided by p_j. The reference scenario is represented by p_i requesting a particular service S_h. We assume that the Service discovery component, which has been described in Section II-A, receives the request of this service from p_i and returns to it a set of nodes $\mathcal{Z}_h = \{p_j \in \mathcal{P} : S_h \in \mathcal{S}_j\}$ that are able to provide the service S_h. For each of this potential service providers $p_j \in \mathcal{Z}_h$, the Service discovery component returns a set of edges $\mathcal{R}_{ij} = \{p_{ij}^a p_{ij}^b\}$, which represents the sequence of social links that constitute the selected path from p_i to p_j in the SIoT. At this point, the Trustworthiness management component is expected to provide the important function of listing the trust level of any node in $\mathcal{Z}_h$. This is the objective of our work.

Fig. 1 provides a simple example of a generic graph $\mathcal{G}$ where: $\mathcal{P} = \{p_1, \cdots p_{10}\}$, with each node capable of providing one or two services, as highlighted in the grey cloud; p_1 is the node that is requesting the service S_{10}, as highlighted in the white cloud; $\mathcal{Z}_{10} = \{p_5\}$ is the set of nodes that can provide the requested service; $\mathcal{R}_{1,5} = \{p_1p_4, p_4p_8, p_8p_5\}$ is the set of edges that constitute the path returned by the Service discovery process for p_1 to reach p_5. In this figure, we also highlight the set $\mathcal{N}_1 = \{p_2, p_3, p_4\}$ of nodes that are friends of p_1 (in blue color). Within note that the set $\mathcal{K}_{1,4} = \{p_2, p_3\}$ of nodes represents the common friends between p_1 and p_4.

B. Trust Models

In such a scenario, we envision two possible models for the implementation of the Trustworthiness management component, based on the dimension of trust semantics [43]:

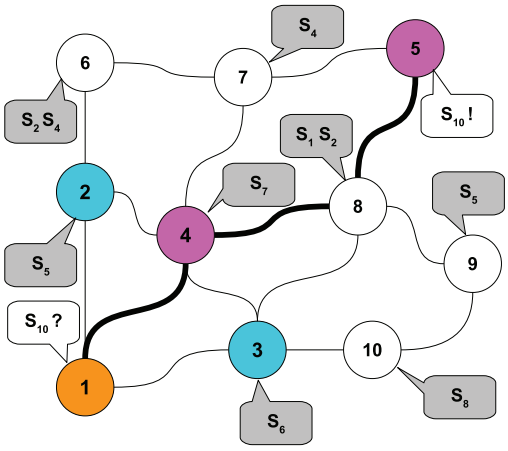


Fig. 1. Representation of the network nodes

1) *Subjective trustworthiness*, derived from a social point of view, where each node p_i computes the trustworthiness of its $\mathcal{N}_i$ friends on the basis of its own experience and on the basis of that of its friends; we refer to this trustworthiness with T_{ij}, i.e., the trustworthiness of node p_j seen by node p_i. If p_i and p_j are not friends, then the trustworthiness is calculated by word of mouth through a chain of friendships.
2) *Objective trustworthiness*, obtained from P2P scenarios, where the information about each node is distributed and stored making use of a DHT (Distributed Hash Table) structure. This information is visible to every node but is only managed by special nodes that we call *Pre-Trusted Objects* (PTOs). We refer to this trustworthiness with T_j, i.e., the trustworthiness of p_j seen by the entire network.

Table II shows how the proposed models match the approaches described in Section II-B in terms of storage, sharing, and processing of the reputation information while Table III summarizes the properties taken from the social networks studies.

The proposed subjective approach shows all the properties typical of trust in online social networks, as described in Section II-C. Indeed, the SIoT can be seen as an application where the objects establish relations and cooperate to provide new services to the users; according to this vision, trust is not related anymore to a particular service, since all the objects in the SIoT try to achieve the same goal and then it can be considered transitive in this scenario. Then, when p_i and p_j are not friends, the transitivity property is exploited. Still, a node uses a composability function to combine the recommendations from the $\mathcal{K}_{ij}$ friends. Moreover, trust is both personal and asymmetric since every object has its own opinion about the other nodes based on its personal experiences, which are different from node to node. These properties have been taken from the past works, whereas other new concepts have been introduced. When building the direct objects opinions, not only are the friendship links taken into account but also the type of relationship. When combining the indirect opinions about a node received from friends, we introduce weights that are

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.

TABLE II
APPROACHES TAKEN FROM THE P2P STUDIES FOR THE MANAGEMENT OF THE REPUTATION INFORMATION ACCORDING TO TABLE I

	Storage	Sharing	Processing
Subjective	Rater-Based	Part	Weighted Average
Objective	Distributed	Global	Weighted Average

TABLE III
PROPERTIES TAKEN FROM THE SOCIAL NETWORKS STUDIES

	Subjective	Objective
Transitivity	X	
Composability	X	X
Personalization	X	
Asymmetry	X	

built on the basis of the node credibility.

In the proposed objective approach, with the use of the Pre-Trusted Objects, the experiences of each node are shared with the entire network, so that there is not transitivity, personalization, and asymmetry. Nevertheless, a composability function is still exploited in order to build a unique trustworthiness value. Similarly to the subjective case, we take the mentioned property of composability from past works as well as the concepts of weighted feedback and credibility to estimate trust values. However, the relationship factor is introduced to estimate the credibility of a released feedback and the centrality is exploited to estimate the total trust value. According to this analysis, we can say that the proposed subjective model derives directly from the approaches adopted for trust management in social networks scenario, whereas the objective model takes the basis from the P2P-related approaches and exploits some properties of the social network area.

C. Basic Trust Elements

Regardless of the particular model implemented, to estimate such reputation we identify seven major factors.

A **feedback system** allows a node p_i to provide an evaluation of the service it has received by the provider p_j. Feedback is represented by f_{ij}^l, which refers to each transaction l and can be expressed either in a binary way ($f_{ij}^l \in \{0,1\}$, i.e., p_i rates 1 if it is satisfied by the service and 0 otherwise), or using values in a continuous range ($f_{ij}^l \in [0,1]$) to evaluate different levels of satisfaction.

The **total number of transactions** between two nodes, indicated by N_{ij}, enables the model to detect if two nodes p_i and p_j have an abnormally high number of transactions.

The **credibility** of node p_i, referred to with C_{ji} (in a subjective way with respect to p_j) or C_i (objective) depending on the model used, represents a key factor in evaluating the information (feedback and trust level) provided by the nodes. This feature can assume values in the range $[0,1]$, with value 1 assigned to nodes with the highest credibility.

The **transaction factor** ω_{ij}^l indicates the relevance of transaction l between p_i and p_j. It is used to discriminate important transactions, $\omega_{ij}^l = 1$, from irrelevant ones, $\omega_{ij}^l = 0$, and can be used as a weight for the feedback. This parameter avoids nodes to build up their trustworthiness with small transactions and then become malicious for an important one. For example, a node builds up its reputation by being honest when providing information about temperature or humidity and then starts to act malicious when asked for a banking transaction. In addition, it can be used to discriminate the functionality of the transactions, so that a node can be trusted only for certain types of service.

To these, we add other two key factors that exploit the main features of the social network among the objects.

One is the **relationship factor** F_{ij} that is related to the type of relation that connects p_i to p_j and represents a unique characteristic of the SIoT. It is useful to either mitigate or enhance the information provide by a friend. Until now, a SIoT implementation does not exist yet, so there are not practical evidences about the weight to assign to each relationship to evaluate the trust. However, the forms of socialization among objects, fully presented in [10], have been devised to represent the human relationships and there are important studies about the connection between relationships and trust. It is a matter of fact that a close friend is more reliable than and acquaintance or a complete stranger [44]. Additionally, many works demonstrate how the relationship and the support from family members are stronger than those received from friends an acquaintances [45], [46]. Moreover, it has been proved from several independent activities that strong ties lead to stronger trust relationship; e.g., in [47] Krackhardt shows how the strong ties imply strong interaction ties for trust and trustworthiness, whereas in [48] Ruef suggests that trust and emotional support are the basic requirements for the creation of strong groups. Based on these considerations, we have assigned different values to F_{ij} on the basis of the relation that connects p_i to p_j (see Table IV). As it will be clear in the following higher values have higher impact on the computed trust. This is a possible setting that we use in this paper on the basis of the following reasoning (but other values can be used as well if justified by different principles). Between two objects that belong to the same owner and then are linked by an OOR, the relationship factor has been assigned with the highest value. According to the mentioned studies, CLOR and the CWOR have been set with only a slightly lower value since are established between domestic objects and objects of the same workplace, respectively. SORs are relationships established between objects that are encountered occasionally (then owned by acquaintances) and for this reason a smaller value is given. Finally, the PORs are the most risky, since they are created between objects of the same brand but that never met and depend only on the model object. If two nodes are tied by two or more relationships, the strongest relation with the highest factor is considered.

The other one is the **notion of centrality** of p_i that is refereed to with R_{ij} (with respect to p_j) in the subjective approach and with R_i in the objective approach. It provides a peculiar information of the social network since if a node has many relationships or is involved in many transactions, it is expected to assume a central role in the network. As described in [49], centrality is "related to group efficiency in problem-solving, perception of leadership and the personal satisfaction

of participants".

TABLE IV
PARAMETERS FOR RELATIONSHIP FACTOR AND COMPUTATION CAPABILITIES

Relationship Factor		
Ownership Object Relationship	OOR	1
Co-Location Object Relationship	CLOR	0.8
Co-Work Object Relationship	CWOR	0.8
Social Object Relationship	SOR	0.6
Parental Object Relationship	POR	0.5
Computation Capabilities		
Class 1	Smartphone, tablet, Set top box	0.8
Class 2	Sensor, RFID	0.2

Another important characteristics of the members of IoT is also considered. The **computation capability** of an object, namely its intelligence I_j. It is a static characteristic of the objects and does not vary over the time. The rational is that we expect a smart object to have more capabilities to cheat with respect to a "dummy" object, leading to riskier transactions. As a reference example, we can consider the case of an air conditioner that request information about the temperature value in a room. Then, the Service discovery process proposes two possible providers: a smartphone and a sensor. Obviously a smartphone is more powerful than a sensor, increasing the chances to act maliciously; accordingly, trusting the sensor instead of the smartphone leads to a safer choice. However the final decision also depends on the other factors used to compute the trustworthiness. To this, we divide the objects into two different classes, and assign to each class a different value, as shown in Table IV: Class1 is assigned to objects with great computational and communication capabilities; to this class belong objects such as smartphones, tablets, vehicle control units, displays, set top boxes, smart video cameras; Class2 is assigned to objects with only sensing capabilities, that is, any object just capable of providing a measure of the environment status and to the RFID-tagged objects.

IV. SUBJECTIVE AND OBJECTIVE MODELS

A. Subjective Trustworthiness

According to the subjective model, each node stores and manages the feedback needed to calculate the trustworthiness level locally. This is intended to avoid a single point of failure and infringement of the values of trustworthiness. We first describe the scenario where p_i and p_j are adjacent nodes, i.e., where they are linked by a social relationship. Then, we considered the other scenarios where they are farer each other in the social network. As already introduced, T_{ij} is the trustworthiness of p_j seen by p_i and is computed as follows

$$T_{ij} = (1-\alpha-\beta)R_{ij} + \alpha O_{ij}^{dir} + \beta O_{ij}^{ind} \tag{1}$$

Accordingly, p_i computes the trustworthiness of its friends on the basis of their centrality R_{ij}, of its own direct experience O_{ij}^{dir}, and of the opinion O_{ij}^{ind} of the friends in common with node p_j ($\mathcal{K}_{ij}$). All these addends are in the range $[0,1]$ and the weights are selected so that their sum is equal to 1 to have T_{ij} is in the range $[0,1]$ as well.

The centrality of p_j with respect to p_i is defined as follows

$$R_{ij} = |\mathcal{K}_{ij}| \Big/ \big(|\mathcal{N}_i| - 1\big) \tag{2}$$

and represents how much p_j is central in the "life" of p_i and not how much it is considered central for the entire network. This aspect helps with preventing malicious nodes that build up many relationships to have high values of centrality for the entire network. Indeed, if two nodes have a lot of friends in common, this means they have similar evaluation parameters about building relationships. This is even more true if the SIoT considers the possibility to terminate a relationship when a very low value of trustworthiness is reached (which is not implemented now in the SIoT). In this way, only the trustworthy relationships are considered in the computation of the centrality and then it can better highlight nodes similarity.

When p_i needs the trustworthiness of p_j, it checks the last direct transactions and determines its own opinion as described in the following

$$O_{ij}^{dir} = \left(\frac{\log(N_{ij}+1)}{1+\log(N_{ij}+1)}\right)(\gamma O_{ij}^{lon} + (1-\gamma)O_{ij}^{rec}) + \\ + \left(\frac{1}{1+\log(N_{ij}+1)}\right)(\delta F_{ij} + (1-\delta)(1-I_j)) \tag{3}$$

This equation tells us that even if no transactional history is available between the two nodes ($N_{ij}=0$), p_i can judge p_j on the basis of the type of relation that links each other and on the computation capabilities. If some interactions already occurred between them, a long-term opinion O^{lon} and a short-term opinion O^{rec} are considered with different weights. Also when N_{ij} is not null the relationship factor and the computation capabilities are considered again, with a weight that decreases as N_{ij} increases.

The long and short-term opinions are computed as follows

$$O_{ij}^{lon} = \sum_{l=1}^{L^{lon}} \omega_{ij}^l f_{ij}^l \Big/ \sum_{l=1}^{L^{lon}} \omega_{ij}^l \tag{4}$$

$$O_{ij}^{rec} = \sum_{l=1}^{L^{rec}} \omega_{ij}^l f_{ij}^l \Big/ \sum_{l=1}^{L^{rec}} \omega_{ij}^l \tag{5}$$

L^{lon} and L^{rec} represent the lengths of the long-term and short-term opinion temporal windows, respectively ($L^{lon} > L^{rec}$), and l indexes from the latest transactions ($l=1$) to the oldest one ($l = L^{lon}$). Moreover, the transaction factor ω_{ij} is used to weight the feedback messages. The short-term opinion is useful when evaluating the risk associated with a node, i.e., the possibility for a node to start acting in a malicious way or oscillating around a regime value after building up its reputation. In fact, the long-term opinion is not sensitive enough to suddenly detect this scenario, since it needs a long time to change the accumulated score.

The indirect opinion is expressed as

$$O_{ij}^{ind} = \sum_{k=1}^{|\mathcal{K}_{ij}|} \big(C_{ik} O_{kj}^{dir}\big) \Big/ \sum_{k=1}^{|\mathcal{K}_{ij}|} C_{ik} \tag{6}$$

where each of the common friends in $\mathcal{K}_{ij}$ gives its own opinion of p_j. In this expression, the credibility values are used to weight the different indirect opinions so that those provided by friends with low credibility impact less than those provided by "good" friends:

$$C_{ik} = \eta O_{ik}^{dir} + (1-\eta) R_{ik} \tag{7}$$

From (7) we see that C_{ik} depends on the direct opinion and on the centrality. Note that the computation of the indirect opinion requires adjacent nodes to exchange information on their direct opinions and list of friends. To reduce the traffic load, it is possible for p_i to request the indirect opinion only to those nodes with a high credibility value.

(2) - (7) allow us to finally compute the subjective trustworthiness in (1). Indeed, for the idea itself of subjective trustworthiness, all the formulas we have shown in this section are not symmetric so that in general $T_{ij} \neq T_{ji}$.

If p_i, that requests the service, and p_j, that provides it, are not adjacent, i.e., are not linked by a direct social relationship, the computation of all the trustworthiness values is carried out by considering the sequence of friends that link indirectly p_i to p_j. The trustworthiness values between no-adjacent nodes T'_{ij} is computed as follows

$$T'_{ij} = \prod_{a,b:p_{ij}^a p_{ij}^b \in \mathcal{R}_{ij}} T_{ab} \tag{8}$$

The requester asks for the trust value of the provider through the route discovered by the Service discovery process (bold route in Fig. 2(a)) and the values are obtained through word of mouth from requester to provider making use of the social relationship described above (green route in Fig. 2(b)). Note that in (8) we are not considering the direct experiences of p_i with p_j. The reason is that in the subjective model, each node stores and manages the feedback and all the information needed to calculate the trustworthiness level of only adjacent nodes. If nodes used (1) to compute the trustworthiness of nodes that are not adjacent, they would need to store a huge amount of data, resulting in a burden on their memory, computation capabilities and battery.

At the end of each transaction, p_i assigns a feedback f_{ij}^l to the service received; in the case p_i and p_j are adjacent, p_i directly assigns this feedback to p_j. Moreover, p_i computes the feedback to be assigned to the friends in $\mathcal{K}_{ij}$ that have contributed to the computation of the trustworthiness by providing O_{ik}^{dir}, so as to reward/penalize them for their advice. According to (9), if a node gave a positive opinion, it receives the same feedback as the provider, namely a positive feedback if the transaction was satisfactory, $f_{ij}^l \geq 0.5$, and a negative one otherwise, $f_{ij}^l < 0.5$; instead, if p_k gave a negative opinion, then it receives a negative feedback if the transaction was satisfactory and a positive one otherwise. Note that the feedback generated by p_i are stored locally and used for future trust evaluations.

$$f_{ik}^l = \begin{cases} f_{ij}^l & \text{if } O_{kj}^{dir} \geq 0.5 \\ 1 - f_{ij}^l & \text{if } O_{kj}^{dir} < 0.5 \end{cases} \tag{9}$$

In the case there is more than one degree of separation, the node p_i assigns a feedback to the adjacent node along the path to the provider. The same assignment is then performed by all the nodes along the path to the provider, unless a node with a low credibility is found (in this case the process is interrupted). With reference to Fig. 2(c), p_1 stores the feedback about p_4 and nodes in $\mathcal{K}_{1,4}$ (i.e., p_2 and p_3) locally. Then it propagates the feedback to p_4, which accepts it only if the credibility of p_1 is high (greater than a predefined threshold). p_4 utilizes it to rate p_8, its last intermediate, and their common friends, in this case only p_3. Then p_4 propagates the feedback to p_8 and so on up to the provider of the service.

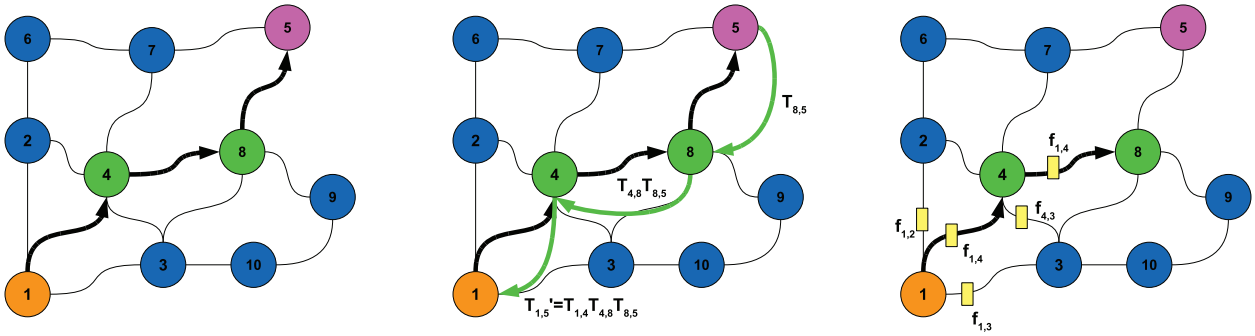
According to this approach, negative feedback is given not only to malicious nodes performing maliciously, but also to malicious nodes that give false references and even to nodes that do not act maliciously but are connected to portions of the network wich are not reliable.

B. Objective Trustworthiness

According to this approach, the values needed to compute the trustworthiness of a node are stored in a distributed system making use of a DHT structure on the network. Several DHT systems are available for this purpose, such as CAN [50], Chord [51], Pastry [52]. In the following, we refer to the Chord system since we have statistics to estimate the performance and open-source tools are commonly available for implementation and simulation.

A DHT system is based on an abstract keyspace, where each node is responsible for a set of keys. An overlay network then connects the nodes, allowing them to find the owner of any given key in the keyspace. To store a file, with a given filename and data, a key for the filename is generated through a hash function (SHA-1 with Chord) and the data and the key are sent to the node responsible for that key. If a node wants to retrieve the data, it first generates the key from the filename and then sends to the DHT a request for the node that holds the data with that key. Chord is a DHT structure that provides good scalability with respect to the network size, since the overhead for information retrieval scales as $O(logM)$ [53], where M are the nodes in the network. It is also very robust to the phenomenon of high churn-rate, i.e., to those nodes moving in and out of the network frequently. This feature is even more important in the IoT settings where the nodes are usually characterized by a more ephemeral connectivity with respect to the scenario of file-sharing.

In our scenario every node can query the DHT to retrieve the trustworthiness value of every other node in the network. In Fig. 3, p_1 queries the DHT to retrieve information about the route discovered by the Service discovery process, namely p_4, p_8, and p_5. To avoid the problem of distributed storage approach where malicious nodes are selected as storage nodes, only special nodes, that we call *Pre-Trusted Objects* (PTOs), are able to store the data about feedback or trustworthiness values. PTOs do not provide any service and are integrated in the architecture; their number is decided based on the number of nodes in the SIoT, so that there is always a PTO available to manage the data. In Fig. 3, p_1 sends the feedback about the transaction to the PTO, that has the role to calculate the new trustworthiness values of the nodes involved in the last



(a) (b) (c)

Fig. 2. Trustworthiness evaluation process for the no-adjacent nodes p_1 and p_5: request of the trust value for a distant node (a), computation of the trust level by multiplying the trust level among adjacent nodes (b) and releasing feedback to the nodes involved in the transaction (c)

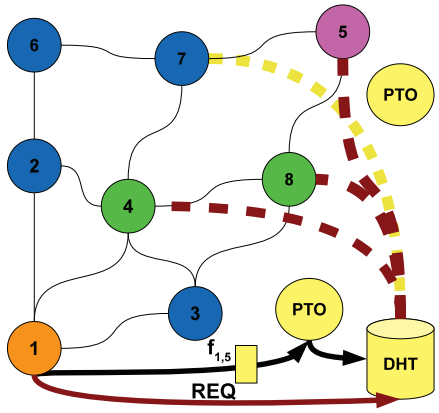


Fig. 3. Objective case: request and store of the trust value

transaction, taking into account the source of the feedback to avoid fake feedback. Then, through the DHT, it generates the key associated with the data and stores it in the node responsible for that key, that is p_7 in this case.

When p_i needs to know the latest trustworthiness value of p_j, it queries the DHT to retrieve it. In this case, there are no direct and indirect opinions since all the nodes can read the trustworthiness value of all other nodes in the DHT, and the trustworthiness is expressed as

$$T_j = (1-\alpha-\beta)R_j + \alpha O_j^{lon} + \beta O_j^{rec} \tag{10}$$

Centrality is now based on the idea that a node is central in the network if it is involved in many transactions, as expressed in the following

$$R_j = (A_j + H_j)/(Q_j + A_j + H_j) \tag{11}$$

where Q_j is the number of times p_j requested a service, A_j is the number of times it acted as an intermediate node in a transaction, and H_j counts how many times it is the provider of a service. A node is considered central if it takes part actively to the SIoT, as either intermediate or provider of the service, in many transactions with respect to all its transactions.

Furthermore, in this approach, the short and long-term opinions are computed considering the feedback received from all the nodes that interacted with p_j

$$O_j^{lon} = \sum_{i=1}^{M}\sum_{l=1}^{L^{lon}} C_{ij}\omega_{ij}^l f_{ij}^l \Big/ \sum_{i=1}^{M}\sum_{l=1}^{L^{lon}} C_{ij}\omega_{ij}^l \tag{12}$$

$$O_j^{rec} = \sum_{i=1}^{M}\sum_{l=1}^{L^{rec}} C_{ij}\omega_{ij}^l f_{ij}^l \Big/ \sum_{i=1}^{M}\sum_{l=1}^{L^{rec}} C_{ij}\omega_{ij}^l \tag{13}$$

To limit the possibility of malicious nodes giving false feedback to subvert the reputation system, every feedback is weighted with the credibility of the node that provides it in addition to the transaction factor. The credibility is defined as follows

$$C_{ij} = \frac{(1-\gamma-\delta)T_i + \gamma(1-F_{ij}) + \delta(1-I_j)}{1+\log(N_{ij}+1)} \tag{14}$$

In this way, nodes with strong relations (i.e., with a small value of the relationship factor), with high computation capabilities or nodes that have a high number of transactions between them, receive a lower credibility. Indeed, this is motivated by the opinion that nodes that fall in this situation (strong relationship links, high intelligence and many interactions) are potential candidates to collusive malicious behavior.

V. Experimental Evaluation

This Section analyses the performance of the proposed models through simulations. Due to the lack of real data concerning some aspects of objects behavior, a complete theoretical analysis of the models performance cannot be achieved. For this reason in Appendix A, we provide a first theoretical analysis for the subjective model case.

A. Simulation Setup

To conduct our performance analysis, we needed mobility traces of a large number of objects. We resorted on the mobility model called *Small World In Motion* (SWIM) [54] to generate the synthetic data and on the real dataset of the

location-based online social network Brightkite obtained from the Stanford Large Network Dataset Collection [55].

The outputs of the SWIM model and the Brightkite dataset are traces of the position of humans. In this paper, instead, we are interested in the mobility of things. Accordingly, we have extended them as follows. We assume that each user owns a set of things that are connected to the SIoT and that during any movement the user carries half of these objects and leaves the others at home. We decided to run the experiments with about 800 nodes, considering that each person owns an average of 7 objects. Objects that stay at home create co-location relationships. Every node is produced by a specific company and is characterized by a model ID; this information is used to build the parental object relationships. The other relationships are created on the basis of the objects (and then owners) movements, mainly taking into account how often objects meet and for how long and where. All the details about the establishment of these social relationships are provided in [6] and [10]. Two different behaviors can be considered in a social network: one is always benevolent and cooperative so that we call the relevant node social nodes. The other one is a strategic behavior corresponding to an opportunistic participant who cheats whenever it is advantageous for it to do so. We call it malicious node and it gives bad services, false references, and false feedback. Its behavior is described by Algorithm 1. Accordingly, it only acts maliciously with objects that it meets occasionally or it has never met, in the same way a person behaves benevolent with close friends and family members and acts maliciously with everyone else (if she/he is malicious). Note that this object behavior is inherited from the owner that authorizes the object interactions according to her/his profile. However, this is true only if the object has enough computational compatibilities to distinguish one relationships from another; otherwise it acts maliciously with everyone. The percentage of malicious nodes is denoted by mp and it is set by default to 25%; we denote with mr the percentage of time in which these nodes behave maliciously (by default $mr = 100\%$).

Algorithm 1 Malicious node behavior

```
if malicious node belongs to Class 1 then
  switch (relationship factor)
  case OOR, CLOR, CWOR:
    act benevolent
  case SOR:
    act benevolent only with close friends
  case POR:
    act maliciously
  default:
    act maliciously
  end switch
end if
if malicious node belongs to Class 2 then
  act malicious with everyone
end if
```

At the start of each transaction, the simulator chooses randomly the node requesting the service and randomly select the nodes that can provide the service, corresponding to a percentage res of the total number of SIoT nodes (by default $res = 5\%$). The malicious node can then be the one requesting the service, the one providing the service or, only in the subjective approach, the one providing its opinion about another node. In the first case, it provides negative feedback to every node involved in the transaction; in the second case, it provides the wrong service and should then received a negative feedback; finally, in the third case, it provides a negative opinion about the other nodes.

TABLE V
SIMULATION PARAMETERS

General parameters

	Parameter	Description	Default
Community setting	M	# of nodes in the SIoT	800
	mp	% of malicious nodes	25 %
	mr	% of transactions a malicious nodes acts malicious	100 %
	res	% of nodes who respond to a transaction request	5 %
Trust computation	L_{lon}	# of transaction in the long-term opinion	50
	L_{rec}	# of transaction in the short-term opinion	5
	n	# of run for each experiment	4

Subjective model parameters

Parameter	Description	Value
α	weight of the direct opinion	0.4
β	weight of the indirect opinion	0.3
γ	weight of the long-term opinion	0.5
δ	weight of the relationship factor	0.5
η	weight of the direct opinion in the credibility	0.7

Objective model parameters

Parameter	Description	Value
α	weight of the long-term opinion	0.4
β	weight of the short-term opinion	0.4
γ	weight of the relationship factor in the credibility	0.3
δ	weight of the intelligence in the credibility	0.3

Table V shows the simulation parameters of the system, and the different weights used with the two approaches. For simplicity, we decided to use a binary feedback system to rate the other nodes according to whether the transaction was satisfactory. For the same reason, we considered all the transactions equally important and we set the transaction factor to 1; finally, each object randomly belongs to one of the computation capabilities classes. To find the optimal system setting we analyzed the models response at varying parameter values. The optimal configuration is provided in Table V. To show the system response at different settings, Table VI displays the transaction success rate when the system has reached the steady-state using the SWIM data. Each row refers to the change of only one parameter while the others keep the optimal setting. As expected, in the subjective approach, the direct opinion has a more impact than the indirect opinion because it is affected by a node own experience, whereas in the objective approach, the most important parameter is the long-term opinion because it takes into account the story of the node. In both the approaches the centrality is the factor that less affects the performance, since it is a slow time variant factor.

TABLE VI
PARAMETERS SETTING

Subjective model values					
$\alpha = 0.1$	0.88	$\alpha = 0.4$	0.93	$\alpha = 0.7$	0.91
$\beta = 0.1$	0.92	$\beta = 0.3$	0.94	$\beta = 0.6$	0.93
$\gamma = 0.2$	0.91	$\gamma = 0.5$	0.93	$\gamma = 0.8$	0.92
$\delta = 0.2$	0.9	$\delta = 0.5$	0.94	$\delta = 0.8$	0.92
$\eta = 0.1$	0.91	$\eta = 0.4$	0.93	$\eta = 0.7$	0.94
Objective model values					
$\alpha = 0.2$	0.89	$\alpha = 0.4$	0.95	$\alpha = 0.6$	0.93
$\beta = 0.2$	0.91	$\beta = 0.4$	0.94	$\beta = 0.6$	0.93
$\gamma = 0.1$	0.92	$\gamma = 0.3$	0.95	$\gamma = 0.7$	0.93
$\delta = 0.1$	0.93	$\delta = 0.3$	0.94	$\delta = 0.7$	0.91

After a node chooses the provider of the service on the basis of the highest computed trustworthiness level, it sends to it the service request. Depending on how the SIoT model is implemented, the service can be delivered either through the nodes that discovered the service, i.e., the social network is also used to transmit the service requests and the responses on top of the existing transport network (overlay structure) or directly relying on the beneath communication network (non-overlay structure). In the first case, a malicious node can interfere with the deliver of the service even if it is in the route from p_i to p_j since it is asked to forward the service request to p_j and the response back p_i. In the latter case, a malicious node can alter the service only if it is the provider.

B. Transaction Success Rate

In this section we present the results for the objective and subjective approaches in the case overlay network is used or not used. We compare the performance of the proposed models with those of the Dynamic Trust Computation of the Tust Value Measure (TVM/DTC) proposed for P2P networks, described in [27]. It relies on a reputation system, which defines a recursive function that uses the trust value of a peer as its feedback credibility measure. We also selected a trust management algorithm for social networks, named TidalTrust [56], which infers trust relationships between people that do not have direct connections through their indirect links. These comparisons are aimed at analyzing the improvements we obtain with respect to the state of the art in the specific reference SIoT scenario. We also show the case in which a trust model is not used.

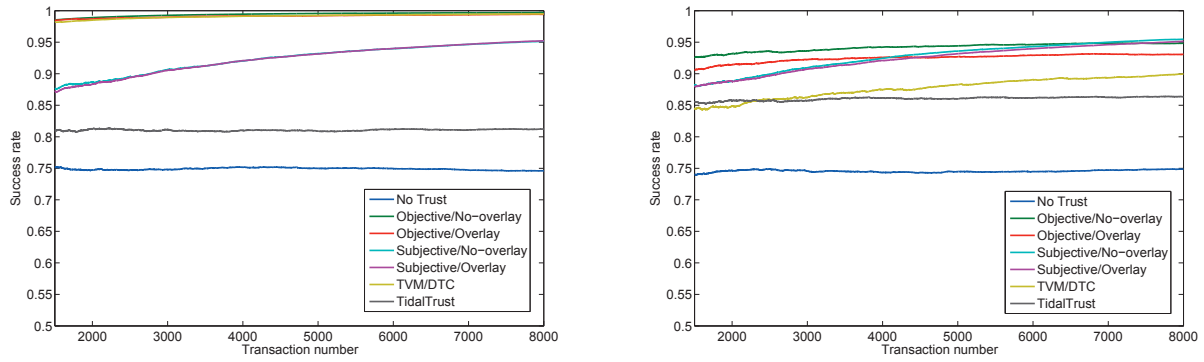
Fig. 4(a) shows the success rate when the malicious nodes only belong to Class2 in the SWIM scenarios. We can observe that the objective model has a faster convergence and presents an higher success rate. This happens since in the objective case, the feedback about a transaction is immediately available to the entire community bringing to a faster converge. Indeed, this model allows for isolating the malicious nodes as fast as 4000 transactions are reached (success rate equal to 99,9%). The subjective approach has indeed a slower transitory, since every node has to build up its own opinion. Still, it's important to point out that this scenario is a very basic one. Malicious Class2 objects are very easy to be identified since they don't behave differently according to the service client, so we can say that this scenario is typical of the P2P networks and then it is favorable for the objective model. Accordingly, the TVM/DTC algorithm presents performance comparable to our objective approach. Differently, Tidal Trust chooses the providers with a weak criteria since a Class2 object acts maliciously with everyone; nevertheless, with respect to the case where no trust algorithm is used, TidalTrust can still achieve significant success rates. Note that since the feedback system is not adopted, the performance don't improve as the number of transactions increases. Since this scenario is a very simplicistic one, we can not observe big differences between the overlay and non-overlay structure; they will be discussed in further simulations.

We now consider the same scenario but with Class1 malicious objects, which can modify their behavior based on the social relationships. Results are shown in Fig. 4(b) for the SWIM scenarios. Still it can be noted as the objective approach converges faster and reaches its steady-state after around 4000 transactions. However, in this case the node trustworthiness is global and mixes the opinions of both the nodes with which it behaved maliciously and the nodes with which it behaved benevolent. This is a drawback only partially addressed by using the relationship factor (see (14)), so that is more difficult to isolate the malicious nodes. With the subjective model each node stores its own trustworthiness data and has its own opinion about the network so that it is clearly more robust towards Class1 malicious objects behavior. As also discussed previously, this approach needs more time to converge but it manages to outperform the objective model after 7000 transactions. With respect to the scenario with Class2 objects, the steady-state performance is slightly worse; this is due to the indirect opinion (see (6)) a node receives from its neighbours, since all the rest of the key data is stored locally. This information depends on the relation between the reference nodes and the service provider, so that can be either positive or negative and can confuse the service requester; however this information is weighted with the credibility of the source node (see (7)), which depends only on the experience of the node that is performing the trustworthiness evaluation.

Another key observation related to the Class1 scenario is that the structure chosen to deliver the service influences the performance. In particular, the use of the overlay structure, where the social network is also used to transmit the service requests and responses, leads to lower performance; indeed, a malicious node can interfere with the delivery of the service because it is in the route from the requester to the provider and it is asked to forward the message. This cannot happen in the non-overlay structure, where a malicious node can alter the service response only when acting as final provider.

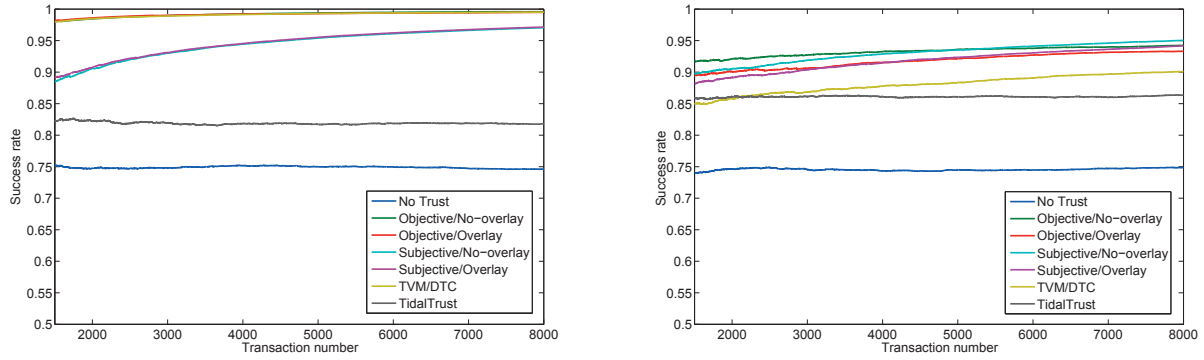
Additionally, it is important to remark that adding the social behavior in the malicious nodes leads to an increase in the TidalTrust performance by almost 5% and a decrease in the TVM/DTC performance by almost 10%. However, it is clear that in the specific SIoT scenario, the well-known techniques for trustworthiness computation studied for either P2P or social networks are not enough to obtain a reliable system, and both our models, subjective and objective, using or not the overlay structure, can outperform these approaches.

Figs. 5(a) and 5(b) show the success rate in the Brightkite



(a) (b)

Fig. 4. Transaction success rate in the SWIM scenario versus the total number of performed transactions with: Class 2 objects (a) and Class 1 objects (b)



(a) (b)

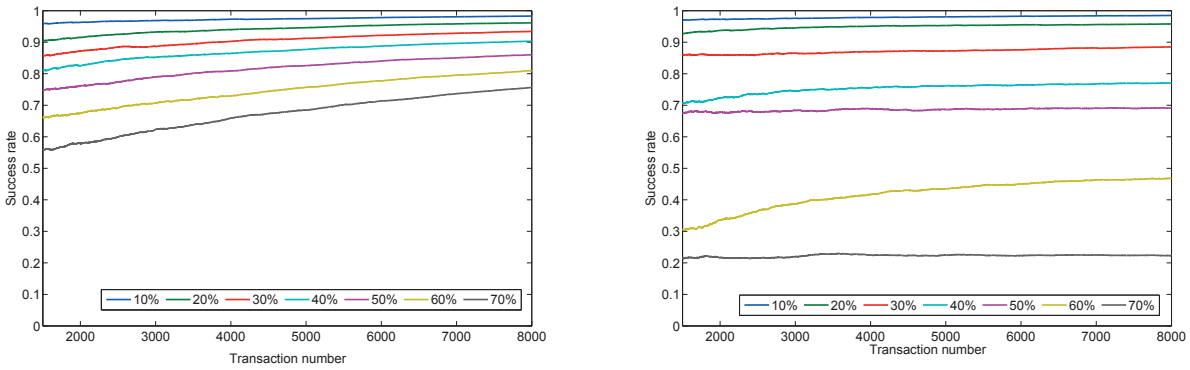
Fig. 5. Transaction success rate in the Brightkite scenario versus the total number of performed transactions with: Class 2 objects (a) and Class 1 objects (b)

scenario when malicious nodes belong to Class2 and Class1, respectively. One of the main differences that can be noted by comparing the results obtained with the two dataset is that in the Brightkite scenario the subjective approach performs slight better than in the SWIM scenario. This is due to the fact that Brightkite is characterized by a shorter network diameter on average with respect to the social graphs generated with SWIM (3 hops instead of 4 hops). Accordingly, in Brightkite every node has more relationships with respect to the SWIM case, which are then exploited by the subjective model that strongly relies on objects direct experience.

We now want to analyze the results at varying percentage of the malicious nodes. Figs. 6(a) and 6(b) refer to the Brightkite scenario with the non-overlay structure and using the subjective and objective approaches, respectively. We note how the subjective approach always converges even with 70% of malicious nodes, since every node has its own vision of the network based on its own experiences. However, the accuracy of this approach decreases, since there is the need for more feedback messages to be collected to cope with the bad recommendations received. Instead, the objective approach is much more sensible to the malicious concentration since every node shares its opinion with the others: with 50% of malicious nodes in the network the performance reaches 0.7; if we further increase the number of malicious nodes, the performance dramatically drops since the opinion of a node is deeply influenced by malicious feedback with appropriate compensation from benevolent ones.

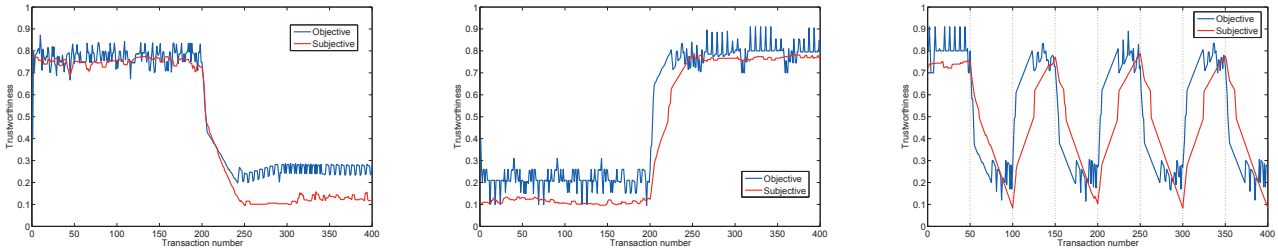
C. Dynamic Behavior

The focus of this set of experiments is to analyze how the proposed approaches work with three different dynamic behaviors of the nodes. In a first scenario, a node builds its reputation and then starts milking it; in a second scenario, a node tries to improve its reputation after having milked it; in a third scenario, the node oscillates between milking and building its reputation. Since we have already analyzed how our algorithms responds to false feedback, we now consider only the malicious behaviors without taking into account nodes providing dishonest feedback. The considered behaviors are independent from the particular networking structure adopted (whether it is overlay or not) or the scenario implemented (whether it is the SWIM or Brightkite scenario) so we only consider the differences between the two subjective and objective models. Fig. 7(a) shows the computed trust value of a node that is milking its reputation; we can observe that, thanks to the short-term window, both algorithms are able to fast adapt to the change in the node behavior. The subjective



(a) (b)

Fig. 6. Transaction success rate in the Brightkite scenario with a non-overlay structure at increasing values of mp: subjective approach (a) and objective approach (b)



(a) (b) (c)

Fig. 7. Dynamic behavior: milking reputation (a), building reputation (b) and oscillating reputation (c)

approach is slightly slower since it has to mediate its opinion with that of its friends, that eventually still trust the malicious node. Similar considerations can be done for a node who is building its reputation as shown in Fig. 7(b), and for a node with an oscillating behavior in Fig. 7(c). These results clearly show how our approaches can cope with dynamic behaviors.

VI. Conclusions

In this paper we have focused on the trustworthiness management in the social IoT by proposing subjective and objective approaches. The major difference between the two methods is that the subjective approach has a slower transitory response, which is particularly evident when dealing with nodes with dynamic behaviors. However, it is practically immune to behaviors typical of social networks, where a malicious person modifies her actions based on the relationships. On the contrary, the objective approach suffers from this kind of behavior, since a node's trustworthiness is global for the entire network and this include both the opinion from the nodes with which it behaved maliciously and the opinion from the nodes with which it behaved benevolent.

As future work, we plan to analyze how the trustworthiness management may also be used to promote social relations, rewarding nodes with a high value of trustworthiness.

Appendix A

Herein we provide an analysis of the performance of the subjective model, whose objective is to discriminate benevolent nodes from malicious ones with the minim error. The resulting trustworthiness formula is made of three additive elements (1), namely the centrality, the direct opinion, and the indirect opinion, each one contributing to isolating malicious nodes.

The subjective centrality measures how much a node is central in another node "life". If we calculate the average centrality of node p_i over all its friendships $\mathcal{N}_i$, we obtain

$$R_i = \frac{\sum_{j=1}^{|\mathcal{N}_i|} \frac{|\mathcal{K}_{ij}|}{\left(|\mathcal{N}_i|-1\right)}}{|\mathcal{N}_i|} = \frac{\sum_{j=1}^{|\mathcal{N}_i|} |\mathcal{K}_{ij}|}{\left(|\mathcal{N}_i|-1\right)|\mathcal{N}_i|} \tag{15}$$

that corresponds to the local clustering coefficient for node p_i, and then gives an indication of how close node p_i's neighbors are to being a clique, i.e. a complete graph.

As there are no models to represent the behavior of the nodes in creating and updating the clusters of friends, we do not have the basis to compute the efficiency of this parameter, but evidences of its capacity to isolate malicious nodes can be found in literature. In [57] the authors state that "trust is to be built based not only on how well you know a person, but also on how well that person is known to the other people in your network" and then they show that, using local clustering for email filtering, it is possible to classify correctly up to 50% of the messages. Moreover, in [58], the authors show how trust networks are highly related to the creation of cluster.

When the nodes start to exchange services, they still do

TABLE VII
PROBABILITY TO MISJUDGE A NODE

Direct opinion

e	μ benevolent	μ malicious	σ^2	error
0.1	0.9	0.1	0.045	$3.15 * 10^{-17}$
0.15	0.85	0.15	0.064	$9.63 * 10^{-7}$
0.2	0.8	0.2	0.08	$1.016 * 10^{-5}$

Indirect opinion

e	μ benevolent	μ malicious	σ^2	error
0.1	0.7	0.3	0.024	$6.56 * 10^{-15}$
0.15	0.675	0.325	0.034	$1.084 * 10^{-5}$
0.2	0.65	0.35	0.043	$1.14 * 10^{-2}$

Direct + Indirect opinion ($\alpha = 0.6$ **and** $\beta = 0.4$)

e	μ benevolent	μ malicious	σ^2	error
0.1	0.82	0.18	0.017	$8.72 * 10^{-77}$
0.15	0.78	0.22	0.024	$2.04 * 10^{-29}$
0.2	0.74	0.26	0.03	$8.31 * 10^{-14}$

not have any information about how much they can trust each other. However, they can rely on the centrality and, for what concerns direct and indirect opinion, on the relationship factor and on the computation capabilities. When N_{ij} becomes high, the dependence of the direct opinion on the relationship factor and the computation capabilities decreases whereas that related to the past transactions increases. The feedback generated for each received service is provided by (9). To simplify the analysis, as done in the simulations, we assume a binary feedback system is used. When analyzing the received service, the client may introduce some errors due to several reasons and mostly because of the intrinsic difficulty in evaluating the quality of the received service. We then introduce probability e that a node gives the wrong feedback, so that the probability to give the correct feedback is $h = 1 - e$. The probability that p_i generates k correct feedback ($f_{ij} = 1$ when p_j is benevolent and $f_{ij} = 0$ when p_j is malicious) over n transactions with p_j, follows a binomial distribution

$$P(k) = \binom{n}{k} h^k (1-h)^{(n-k)} \tag{16}$$

Note that if we consider feedback having the same weights, the long term and short term opinions $O_{ij}^{lon/rec} = k$ if p_j is benevolent and $O_{ij}^{lon/rec} = 1 - k$ if p_j is malicious. Accordingly, these follow a binomial distribution as well, where the expected value is h if node p_j is benevolent, and $1 - h$ if it is malicious, and the variance is $h(1 - h)$. This distribution can be approximated with a gaussian one (when $n > 30$) with the same variance and average values. When adding the two contributions from the short and long term opinions, considering $\gamma = 0.5$ as in the simulations, we obtain that the direct opinion is still a gaussian distribution with the same mean value ($\mu_b = p$ and $\mu_m = 1 - p$ based on the behavior of node p_j) and a variance equals to $h(1 - h)/2$.

To calculate the distribution of the indirect opinion, we assume for simplicity that the credibility for all the nodes is the same; in this case, it is the sum of gaussian-distributed variables, so it follows a gaussian distribution as well. Considering that x% of the nodes are malicious, the average value for the indirect opinion is $(1 - 0.x)\mu_{b,m} + 0.x\mu_{m,b}$ while its variance is $\sigma^2 / |\mathcal{K}_{ij}|$.

Using the $erfc$ function to calculate the error when estimating the trustworthiness of a node, we obtain the results shown in Table VII for different values of the error probability and $x = 25\%$. Both the parameters can achieve low error probability. Indeed, the direct opinion is the parameter that most affects the trustworthiness calculation, and that leads to the smallest errors. However, when services start to circulate in the network, the first parameter that varies and gives actual information about the trustworthiness of a node is the indirect opinion. This happens because, if node p_i wants to evaluate the trustworthiness of node p_j, it is simply more probable that it can obtain information from one of the common friends $\mathcal{K}_{ij}$ than from a direct transition between p_i and p_j. Moreover, with the combination of these two parameters, it is possible to achieve more reliable results than using only one of them.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787 – 2805, 2010.
[2] P. Mendes, "Social-driven internet of connected objects," in *Proc. of the Interconn. Smart Objects with the Internet Workshop*, 2011.
[3] L. Ding, P. Shi, and B. Liu, "The clustering of internet, internet of things and social network," in *KAM Symposium, 2010*, 2010.
[4] D. Guinard, M. Fischer, and V. Trifa, "Sharing using social networks in a composable web of things," in *PERCOM Workshops, 2010*.
[5] E. A. K. amd N. D. Tselikas and A. C. Boucouvalas, "Integrating rfids and smart objects into a unified internet of things architecture," *Advances in Internet of Things*, vol. 1, no. 1, pp. 5–12, 2011.
[6] L. Atzori, A. Iera, and G. Morabito, "Siot: Giving a social structure to the internet of things," *Communications Letters, IEEE*, vol. 15, 2011.
[7] J. Surowiecki, *The wisdom of crowds*. Doubleday, 2004.
[8] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011.
[9] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "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*, 2012, pp. 18–23.
[10] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," *Computer Networks*, 2012.
[11] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "Trm-iot: A trust management model based on fuzzy reputation for internet of things." *Comput. Sci. Inf. Syst.*, vol. 8, no. 4, pp. 1207–1228, 2011.
[12] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Hierarchical trust management for wireless sensor networks and its application to trust-based routing," in *ACM Symposium on Applied Computing*, 2011.
[13] Y. Liu, Z. Chen, F. Xia, X. Lv, and F. Bu, "A trust model based on service classification in mobile services," in *Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on Int'l Conference on Cyber, Physical and Social Computing (CPSCom)*, 2010, pp. 572–577.
[14] F. Bao and I.-R. Chen, "Trust management for the internet of things and its application to service composition," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a*, 2012, pp. 1–6.
[15] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," *Commun. ACM*, vol. 43, pp. 45–48, 2000.
[16] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th international conference on World Wide Web*, 2003.
[17] A. A. Selcuk, E. Uzun, and M. R. Pariente, "A reputation-based trust management system for p2p networks," in *Proceedings of the 2004 IEEE International Symposium on Cluster Computing and the Grid*. IEEE Computer Society, 2004, pp. 251–258.
[18] R. Sherwood, S. Lee, and B. Bhattacharjee, "Cooperative peer groups in nice," *Comput. Netw.*, vol. 50, pp. 523–544, 2006.
[19] E. Adar and B. A. Huberman, "Free riding on gnutella," 2000.

[20] M. Feldman, K. Lai, and J. Chuang, "Quantifying disincentives in peer-to-peer networks," in *1st Workshop on Economics of Peer-to-Peer Systems*.

[21] R. Jurca and B. Faltings, "An incentive compatible reputation mechanism," in *Proceedings of the second international joint conference on Autonomous agents and multiagent systems*. ACM, pp. 1026–1027.

[22] S. Marti and H. Garcia-Molina, "Identity crisis: Anonymity vs. reputation in p2p systems," in *Proceedings of the 3rd International Conference on Peer-to-Peer Computing*. IEEE Computer Society, 2003, p. 134.

[23] R. Zhou, K. Hwang, and M. Cai, "Gossiptrust for fast reputation aggregation in peer-to-peer networks," *IEEE Trans. on Knowl. and Data Eng.*, vol. 20, pp. 1282–1295, 2008.

[24] Z. Liang and W. Shi, "Enforcing cooperative resource sharing in untrusted p2p computing environments," *Mob. Netw. Appl.*

[25] Y. Wang and J. Vassileva, "Bayesian network-based trust model," in *Proceedings of the 2003 IEEE/WIC International Conference on Web Intelligence*, ser. WI '03. IEEE Computer Society, 2003, pp. 372–.

[26] B. Yu, M. P. Singh, and K. Sycara, "Developing trust in large-scale peer-to-peer systems," in *Proceedings of First IEEE Symposium on Multi-Agent Security and Survivability*, 2004, pp. 1–10.

[27] L. Xiong and L. Liu, "Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING*, vol. 16, pp. 843–857, 2004.

[28] B. E. Commerce, A. Jsang, and R. Ismail, "The beta reputation system," in *In Proceedings of the 15th Bled Electronic Commerce Conference*.

[29] Z. Despotovic and K. Aberer, "Maximum likelihood estimation of peers' performance in p2p networks," 2004.

[30] T. DuBois, J. Golbeck, and A. Srinivasan, "Predicting trust and distrust in social networks," in *Privacy, security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom)*. IEEE, 2011, pp. 418–424.

[31] B. Carminati, E. Ferrari, and J. Girardi, "Trust and share: Trusted information sharing in online social networks." in *ICDE*. IEEE Computer Society, 2012, pp. 1281–1284.

[32] A. Jøsang, "Artificial reasoning with subjective logic," in *Proceedings of the Second Australian Workshop on Commonsense Reasoning*, 1997.

[33] G. Liu, Y. Wang, and L. Li, "Trust management in three generations of web-based social networks," in *Proceedings of the 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing*, ser. UIC-ATC '09. IEEE Computer Society, 2009, pp. 446–451.

[34] P. W. Fong, "Relationship-based access control: protection model and policy language," in *Proceedings of the first ACM conference on Data and application security and privacy*. ACM, 2011, pp. 191–202.

[35] B. Carminati, E. Ferrari, and M. Viviani, "A multi-dimensional and event-based model for trust computation in the social web," in *Social Informatics*. Springer, 2012, pp. 323–336.

[36] J. A. Golbeck, "Computing and applying trust in web-based social networks," Ph.D. dissertation, 2005.

[37] J. Golbeck and J. Hendler, "Inferring binary trust relationships in web-based social networks," *ACM Trans. Internet Technol.*

[38] A. Jøsang, R. Hayward, and S. Pope, "Trust network analysis with subjective logic," in *Proceedings of the 29th Australasian Computer Science Conference*. Australian Computer Society, 2006, pp. 85–94.

[39] A. Jøsang and S. Pope, "Semantic constraints for trust transitivity," in *Proceedings of the 2nd Asia-Pacific conference on Conceptual modelling*. Australian Computer Society, Inc., 2005, pp. 59–68.

[40] B. Christianson and W. S. Harbison, "Why isn't trust transitive?" in *Proceedings of the International Workshop on Security Protocols*. Springer-Verlag, 1997, pp. 171–176.

[41] A. P. Fiske, "The four elementary forms of sociality: framework for a unified theory of social relations," *Psychological review*.

[42] L. E. Holmquist, F. Mattern, B. Schiele, P. Alahutha, M. Beigl, and H. Gallersen, "Smart-its friends: A technique for users to easily establish connections between smart artefacts," in *Proc. of ACM UbiComp'01*.

[43] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decis. Support Syst.*

[44] R. Ashri, S. Ramchurn, J. Sabater, M. Luck, and N. Jennings, "Trust evaluation through relationship analysis," in *Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems*. ACM, 2005, pp. 1005–1011.

[45] M. Procidano and K. Heller, "Measures of perceived social support from friends and from family: Three validation studies," *American journal of community psychology*, vol. 11, no. 1, pp. 1–24, 1983.

[46] G. Zimet, N. Dahlem, S. Zimet, and G. Farley, "The multidimensional scale of perceived social support," *Journal of personality Assessment*, vol. 52, no. 1, pp. 30–41, 1988.

[47] D. Krackhardt, "The strength of strong ties: The importance of philos in organizations," *Networks and organizations: Structure, form, and action*, vol. 216, p. 239, 1992.

[48] M. Ruef, "Strong ties, weak ties and islands: structural and cultural predictors of organizational innovation," *Industrial and Corporate Change*, vol. 11, no. 3, pp. 427–449, 2002.

[49] L. Freeman, "Centrality in social networks conceptual clarification," *Social networks*, vol. 1, no. 3, pp. 215–239, 1979.

[50] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker, "A scalable content-addressable network," *SIGCOMM Comput. Commun. Rev.*, vol. 31, pp. 161–172, 2001.

[51] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," *SIGCOMM Comput. Commun. Rev.*, vol. 31, pp. 149–160, 2001.

[52] A. I. T. Rowstron and P. Druschel, "Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems," in *Proceedings of the IFIP/ACM International Conference on Distributed Systems Platforms Heidelberg*. Springer-Verlag, 2001, pp. 329–350.

[53] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," *SIGCOMM Comput. Commun. Rev.*, vol. 31, no. 4, pp. 149–160, 2001.

[54] A. Mei and J. Stefa, "Swim: A simple model to generate small mobile worlds," in *INFOCOM 2009, IEEE*, 2009, pp. 2106 –2113.

[55] J. Leskovec, "Stanford large network dataset collection." [Online]. Available: http://snap.stanford.edu/data/

[56] J. Golbeck, "Personalizing applications through integration of inferred trust values in semantic web-based social networks," *W8: Semantic Network Analysis*, p. 15, 2008.

[57] O. P. Boykin and V. Roychowdhury, "Personal Email networks: an effective anti-spam tool," *Condensed Matter cond-mat/0402143*, 2004.

[58] W. Yuan, D. Guan, Y.-K. Lee, S. Lee, and S. J. Hur, "Improved trust-aware recommender system using small-worldness of trust networks," *Knowledge-Based Systems*, vol. 23, no. 3, pp. 232–238, 2010.

Michele Nitti was awarded with the Master Degree in Telecommunication Engineering with full marks in 2009 at the University of Cagliari. From January to July 2009 he was an Erasmus student at the Cork Institute of Technology. In 2010 he worked for a year as a researcher at the National Interuniversity Consortium for Telecommunications (CNIT) at Cagliari, on the development of models for network connectivity in mobile ad hoc network. He is currently studying as a PhD student in Electronic and Computer Engineering at the University of Cagliari. His main research interests are on Internet of Things (IoT), particularly on the creation of a network infrastructure to allow the objects to organize themselves according to a social structure.

Roberto Girau received the M.S. degree in Telecommunication Engineering from the University of Cagliari, Italy in 2012 , discussing the thesis Trustworthiness management in the social Internet of Things. Since graduation, he has been working as researcher at the Department of Electrical and Electronic Engineering of the University of Cagliari, developing an experimental platform for the social Internet of Things. His main research areas of interest are IoT with particular emphasis on its integration with social networks, software engineering.

Luigi Atzori is assistant professor at the University of Cagliari (Italy) since 2000. His main research topics of interest are in service management in next generation networks, with particular attention to QoS, service-oriented networking, bandwidth management and multimedia networking. He has published more than 100 journal articles and refereed conference papers. Dr. Atzori has received the Telecom Italia award for an outstanding MSc thesis in Telecommunication and has been awarded a Fulbright Scholarship (11/2003-05/2004) to work on video streaming at the Department of Electrical and Computer Engineering, University of Arizona. He is senior member of IEEE and vice-chair of the IEEE Multimedia Communications Committee (MMTC). He has been the editor for the ACM/Springer Wireless Networks Journal and guest editor for the IEEE Communications Magazine, Monet Journal and Signal Processing: Image Communications journals.