ResIoT: An IoT Social Framework Resilient to Malicious Activities

Giancarlo Fortino*, Fabrizio Messina†, Domenico Rosaci‡, Giuseppe M. L. Sarné §
*Depart. DIMES, Univ. of Calabria, Via P. Bucci, 87036 Rende (CS), Italy, giancarlo.fortino@unical.it
†Depart. DMI, Univ. of Catania, Viale Andrea Doria 6, 95126 Catania (CT), Italy, messina@dmi.unict.it
‡Depart. DIIES, Univ. Mediterranea, Loc. Feo di Vito, 89122 Reggio Cal. (RC), Italy, domenico.rosaci@unirc.it
§Depart. DICEAM, Univ. Mediterranea, Loc. Feo di Vito, 89122 Reggio Cal. (RC), Italy, sarne@unirc.it

***Abstract*—The purpose of the next Internet of Things (IoT) is that of making available myriad of services to people by high sensing intelligent devices capable of reasoning and real time acting. The convergence of IoT and Multi-Agent Systems provides the opportunity to benefit from the social attitude of agents in order to perform Machine-to-Machine cooperation among smart entities. However, the selection of reliable partners for cooperation represents a hard task in a mobile and federated context, especially because the trustworthiness of devices is largely unreferenced. The issues discussed above can be synthesized by recalling the well known concept of *social resilience* in IoT systems, i.e. the capability of an IoT network to resist to possible attacks by malicious agent that potentially could infect large areas of the network, spamming unreliable information and/or assuming unfair behaviors. In this sense, social resilience is devoted to face malicious activities of software agents in their social interactions, and do not deal with the correct working of the sensors and other information devices. In this setting, the use of a reputation model can be a practicable and effective solution to form local communities of agents on the basis of their social capabilities. In this paper, we propose a framework for agents operating in an IoT environment, called ResIoT, where the formation of communities for collaborative purposes is performed on the basis of agent reputation. In order to validate our approach, we performed an experimental campaign by means of a simulated framework, which allowed us to verify that, by our approach, devices have not any economic convenience to performs misleading behaviors. Moreover, further experimental results have shown that our approach is able detect the nature of the active agents in the systems (i.e., honest and malicious), with an accuracy of not less than 11% compared to the best competitor tested and highlighting a high resilience with respect to some malicious activities.**

***Index Terms*—Group Formation, IoT, Multi-agent System, Reputation**

I. Introduction

In the "Internet of Things" (IoT) [1] the main actors are physical or virtual "smart" entities provided with embedded computational, sensing and communication capabilities [2]. Such characteristics allow to realize smart environments where potentially useful and attractive services can be made available to other IoT devices and/or humans in an every time and everywhere fashion [3], [4]. To this aim, a recent trend is represented by adaptive forms of cooperation among smart objects [5] to compose more and more sophisticated and complex services [6], [7].

IoT social abilities enable various different services in a scalable and pervasive way in smart IoT-based environments. To this purpose, an attractive and disruptive opportunity is provided by the convergence of IoT and Multi-Agent Systems (MAS) technologies. Indeed, by associating smart IoT objects with software agents working on their behalf [8], [9], it is possible to exploit the social attitude of software agents to interact and cooperate [10].

Such a possibility is quite interesting in presence of a great number of federated IoT environments [11], [12] and IoT devices that migrate through them [8], [13]. In particular, the possibility for an IoT object to move across several administrative domains is very appealing but, on the other hand, the number of potentially partners could be really huge. To profitably cooperate with other IoT smart objects (i.e., the associated agents) suitable information about potential partners are needed for selecting the most "effective" and "reliable" among them [14].

We may take into account, for instance, a smart urban mobility scenario characterized by vehicle-to vehicle (V2V) interactions, for instance exchanging traffic information [15]. This scenario is characterized by a large population of federated smart devices, where each environment can host agents coming from other environments (e.g., another city). Therefore, any agent associated with a vehicle may ask for information for some potential partners, and it is highly probable that its own provider can be unreferenced with respect its reliability and there exists the risk of obtaining an unsatisfactory service.

The choice of a partner will impact on the quality of the interactions having place among cooperating objects, and the resulting "satisfaction" that each object perceives [16] will change accordingly. This aspect is particularly important in presence of complex tasks and/or economic interests (e.g., when the cooperation or a service is provided for pay) [17].

A common approach adopted in human contexts – in order to select a reliable partner – consists of asking to some reliable agents for information. However, this approach is difficult to be adopted because the probability for an agent to interact with partners having an unreferenced reliability is not neglecting and the agent should rely on the global reputation the whole community has in the other agents [18].

However, similarly to human communities, a possible approach to tackle the problem of selecting the most suitably partners consists in exploiting some type of local social structure among the agents on the basis of one or more criteria [19], [20]. The formation of such social structures, as agent teams,

denotes the existence of a reasonable mutual expectancy among team members for positive social relationships.

Furthermore, considering the mobile nature and the high heterogeneity of the involved IoT objects, the common strategy of forming teams based on structural and/or semantic similarities among the team members (e.g. similar interests, tastes and/or preferences) is not easily exploitable [21]. Therefore, different criteria should be considered.

In the scenario above described this context, it becomes important to consider the dynamics of the processes designed to drive the formation and the evolution of social groups [22], [23]. To this end, a suitable approach is represented by a team formation process where their members have high levels of mutual trustworthiness [24], [4] for allowing the selection of reliable partners also by considering possible cheating activities perpetrated by malicious agents. The issues discussed above can be synthesized by recalling the well known concept of *social resilience* in IoT systems. Social resilience is a desirable property of distributed, large-scale IoT systems [25], [26], that can be defined as the capability of an IoT network to resist to possible attacks by malicious agents able to infect large areas of the network, spamming unreliable information and/or assuming unfair behaviors. According to this definition, an IoT system is resilient to malicious attacks if it implements suitable strategies devoted to individuate suspect agents, isolate them and discourage their unfair activities. In this sense, social resilience is devoted to face malicious activities of software agents in their social interactions, and do not deal with the correct working of the sensors and other information devices. Note that from hereafter we will use the short term resilience to indicate this notion of social resilience.

A. Our proposal: An IoT social framework resilient to malicious activities

In this paper we present a new reputation based framework for IoT agents, called **Res**ilient **IoT** (ResIoT), having the social capability to form agent local communities. ResIoT has been specifically designed to be resilient to a certain kind of malicious attacks. ResIoT has been conceived for all those IoT scenarios formed by federated environments in which heterogeneous devices, provided of limited computational, storage and power resources, are free to move between domains and where cooperation exploits the formation of social structures based on the widespread reputation in the network.

The main contributions provided in this paper as the following:

- The first contribution provided by our framework consists of proposing the use of a new agent reputation measure, called *reputation value* (RV) obtained by considering the feedback released by the agents during their activities and implementing some suitable countermeasures to avoid collusive and misleading activities [27]. Such reputation scores are used for supporting the formation of local communities of agents in which agents are grouped as teams on the basis of their RVs by means of an apposite community formation algorithm (see Section V-A).
- A second contribution provided by our proposal is that of the capability of filtering some of the interactions for building the RV of an agent. In other words, by our model, we are able to consider only the interactions satisfying certain requirements, named "Characterizing Interactions" that will be described in detail in Section IV. Such a peculiarity allows to the reputation model of ResIoT to identify the nature (e.g., honest or malicious) of the agents more quickly (i.e., in very narrow number of interactions) than other reputation systems (see Section VI-A).
- A further third contribution of our work is represented by the introduction of a competitive mechanism capable of increasing the overall reputation value of each agent community by promoting improvements in agent members reputation and making not profitable for the agents to cheat.

It is important to note that our approach introduce a necessary level of complexity in the IoT system, motivated from the exigency of accurately modeling the relations of trustworthiness among the agents, on one hand, and that of implementing an effective strategy to form teams of agents, on the other hand. These two necessities need to be addressed as apposite conceived, not trivial approaches.

Note as in the following, we will refer exclusively to mobile IoT devices without this means a loss of generality. Moreover, reasonably we assume that each agent requiring a service will interact only inside the federated environment where it is currently joined with. In such a scenario, an IoT object can receive a services for free exclusively from its "friend" agents (i.e., the IoT smart objects joined with the same agent team), otherwise it has to pay for the service.

B. Structure of the paper

Section II reviews the relevant related work found in the literature. Section III introduces the proposed IoT framework. Section IV describes our reputation model. Section V discusses how we planned the experiments, while section VI presents and discusses the experimental results. Finally, Section VII discusses the main results and our conclusions.

II. Related Work

The literature on trust and reputation systems is rather wide: trust-based approaches have been adopted in a large number of different scenarios [28], [29].

The context represented by the distributed Internet of Things, where there is not a central entity acting as service hub as well as indexing [25] – although the Cloud still represent a viable solution for computation intensive tasks [30] – is particularly interesting for its distributed nature. Trust and reputations systems, as well as group (i.e., teams) formation can play a crucial role in this scenario: indeed the distributed Internet of Things is naturally exposed to a large number of potential risks due to cheating and/or inappropriate behaviors with respect to centralized environments [25]. While ciphering techniques are designed for authentication and privacy issues [31], trust and reputation systems are designed to provide an effective support in estimating potential counterparts with respect to their trustworthiness. Indeed, any potential partner

or service customer would know how much the community (or a subset of it) trusts a certain peer [32]. In particular, trust is generally obtained by exploiting past direct agents experiences (reliability) and/or opinions provided by others (reputation). Reliability and reputation are often arranged in a unique measure (for instance [33], [34], [35]).

A. Trust and reputation models.

Several proposals concerning trustworthiness measures have been presented in the past. Probably the most known in the commercial environment is that of eBay [36]. The eBay reputation system allows members (customers and sellers) leave feedback about interactions with each other. The system is transaction based, so that in order to leave feedback for each other, two members must have completed a transaction. Once the auction is complete, the buyer and the seller can rate each other's performance with either a positive, a neutral or a negative feedback. Members' reputation scores are computed as the count of distinct users who gave positive feedback minus the count of those who gave negative feedback. Another well known example of reputation system is SPORAS [37], that was introduced to improve online reputation models, and it is meant for a loosely connected environment, in which users share the same interest. The reputation value is calculated by aggregating users' opinions, and the two most recent users are considered for gathering the rating values. The system measures the reliability of each interaction based on the standard deviation of reputation. It is a model which considered reliability in its rating method.

A few recent works, as [38] focus on achieving reliable broadcast under various kind of failures by using the notion of trust to improve the performance of reliable broadcast. An example of a recent reputation system, we can cite that presented in [39], appositely conceived for IoT scenarios. This is a novel trust assessment framework for the security and reputation of cloud services, that enables the trust evaluation of cloud services in order to ensure the security of the cloud-based IoT context via integrating security-and reputation-based trust assessment methods. The security-based trust assessment is realized using cloud-specific security metrics to evaluate the security of a cloud service. Moreover, a mechanism of feedback ratings on the quality of cloud service is used in the reputation-based trust assessment method in order to evaluate the reputation of a cloud service. Trust Computation Model (TCM) is based on a set of required prior knowledge to making a trust decision [40]. Such knowledge includes information about other agents' knowledge base, and the performed interactions during the current task. A key feature of TCM is that it considers how much knowledge one should have about the trustee agents in order to make a trust decision. TCM model introduces a direct trust measure based on three concepts: familiarity, similarity and past experience, whereas indirect trust is defined based on recommendations.

ReGret [41] is a decentralized environment in which social relations among agents assumes a key role. ReGreT manages reputation considering three different dimensions: individual, social and ontological. Moreover, its reputation mechanism includes three specialized reputation types, differentiated by the information sources: witness, neighborhood, and system reputations. After every interaction, each user rates its partner's performance, and the ratings are saved in a local database. An agent applies the information of the stored ratings to evaluate another agent's trust by querying its local database. Recently, the Trust and Reputation Interaction Model (TRIM) has been proposed [42], to model an interacting agent environment with malicious agents along with an underlying TRS. TRIM, whose runtime behavior can be specified as an infinite state homogeneous Markov Decision Process (MDP) tree, has expressive power to cover a wide range of TRSs and is able to define advanced complicated attacks.

B. IoT, trust and social networking.

With the growth of the IoT world in terms of number of devices and novel applications, the recent literature reports some efforts to design trust and reputation models for IoT [43], [44], [45].

The model proposed in [46] provides a dynamic trust management protocol which is integrated in the IoT scenario with a trust-based service composition. This work highlights the "social nature" of relationships occurring between IoT devices.

One more step towards social (IoT) networking is represented by the work described in [47], which represents a trust system designed to follow the evolution of social relationships for adapting itself to the trust variations.

BETaaS [48] describes a trust model aimed at monitoring things and behaviors for evaluating their reliability. Its trust model considers different aspects among which security, QoS, scalability, availability and gateways reputation. A further work is described in [49] where a particular attention is given to the heterogeneous skills of devices in different cooperative tasks in a distributed IoT system. First, second-hand information and observations are exploited by peers in order to collect trustworthiness information, matching demand and offer for services, learn from past experiences and provide recommendations about the trustworthiness of the other devices active within the community.

C. IoT, trust and team formation.

Smart devices can form teams of like-minded peers by means of their social interactions and mutual trust evaluation [50]. Nevertheless, a few, very important aspects, such as scalability (e.g., billions of devices) and countermeasures against bad-mouthing attacks, have to be considered when forming trust-based groups in IoT environments. To this regards, [51] proposes an approach for scalable trust-based IoT clustering as well as an intelligent method for countering bad-mouthing attacks on trust systems. The authors also take into account trust computation and trust-based migration of IoT nodes from one cluster to another. The convergence among IoT, software agents and cloud computing to form groups of agents (each one associated with an IoT device and living on the cloud) has been recently studied in [4], where an algorithm to form agent groups on the basis of information

about reliability and reputation collected by the agents is presented.

D. Trust-based resilience in IoT networks.

Resilience is a desirable property of distributed, large-scale IoT systems [25]. In [52] the authors focus on the concept of resilience for IoT systems with particular emphasis to attacks that potentially could destroy large areas of the network in the context of smart cities. Since one of the most peculiar aspect of smart cities is represented by the large heterogeneity of coexisting protocols and mechanisms [53], the authors propose to adopt the concept of islands of resilience with respect to all the critical services (e.g. DNS, caching, CDNs) such that they can continue to operate even in presence of severe attacks.

The work described in [54] discusses a class of distributed constrained optimization problems in power systems, where the goal is to optimize the sum of all agents' local convex objective functions over a general unbalanced directed communication network. The author propose a novel distributed primal-dual augmented (sub) gradient algorithm which utilizes a row-stochastic matrix and employs uncoordinated step-sizes, and yet exactly converges to the optimal solution over a general unbalanced directed communication network. The authors also present an explicit analysis for the convergence rate of the proposed algorithm, as well as three case studies to solve two practical problems in power systems.

The resilience requirement in IoT networks is also discussed in [26]. This study investigated about the classic observe-analyze-adapt loop by addressing problems involving devices, networks, and applications, and discusses the problem by illustrating two different projects described by the authors. Finally, a middleware framework for improving resilient communications between devices and services is proposed, with a focus on a scalable resilient multi-protocol data exchange and distributed applications.

The work in [55] is an attempt to provide an in depth analysis about the IoT platforms from the communication architecture viewpoint in order to evaluate the effects of communication anomalies. The authors also propose to adopt hybrid network infrastructures composed of Software Defined Networking (SDN) and redundant non-SDN segments to improve the network resilience.

Resilience for Cloud-based IoT applications has been addressed in [56]. The authors took into account the wide range of applications (warfare, agriculture and delivery) related to Aerial Vehicles (drones). In this scenario vulnerabilities may cause heavy losses. The authors proposed a distributed solution by adopting blockchain technology [57], [58] to securing drone data collection and communication in combination with a public blockchain for provisioning data integrity and cloud auditing. The authors have shown that the proposed system provides a good resilience with acceptable overhead and scalability for a large number of drones.

A few works addressed the problem of resilience in IoT networks by means of trust-based approaches. In [59] the authors considered a local-area networks with a number of IoT devices having limited processing capabilities and face energy constraints, which have to provide the needed security mechanisms. They propose a trust-based routing solution formed by a trust-based approach for managing the reputation of every node of the IoT network which is based on the emerging Routing Protocol for Low power and Lossy networks (RPL). The approach was simulated by the authors in order to measure the level of resilience in presence of specific attacks.

An interesting work is that described in [60], that deals with a general class of distributed constrained optimization problems over a multiagent network, where the global objective function is represented by the sum of all local objective functions. In particular, each agent in the network is aware of its own local objective function. Moreover, it is is restricted to a global nonempty closed convex set. The authors consider a scenario on which the communication of the whole multiagent network is represented as a sequence of time-varying general unbalanced directed graphs. They propose a new distributed projection sub-gradient algorithm which can be adopted to solve the problem on the time-varying general unbalanced directed graphs. Moreover, it does not need each agent to know its in-neighbors out-degree. Simulation results prove the substantiate feasibility of the proposed algorithm and correctness of the theoretical findings. In spite of the problem considered in these work are currently behind the focus of our work, we will consider them in a future work.

A recent work of Liu et Al. [61] addresses the problem of resilience in large IoT systems. The role of reputation systems is discussed to obtain effective countermeasures for securing Machine-to-Machine (M2M) communications against various types of attacks. They proposed a system named M2MTrust where two novel trust-metrics are introduced: pairwise similarity based feedback and credibility as well as threshold-controlled trust propagation. The former is used to compute the direct trust coming from M2M relationships, while the latter is used to block the trust propagation from good nodes to malicious ones. The authors proved that the designed system is resilient with respect to attacks of different nature and it shows good performance also in the presence of dishonest feedback.

III. The proposed Framework

The considered IoT framework (depicted in Figure 1) includes a large number of heterogeneous IoT devices having limited resources. Agents can mutually cooperate to reach their respective targets at the best. To promote such cooperating activities, we assume that each device is assisted by a hosted software agent in order to exploit its "social" skills by working on the behalf of its device. Each agent can interact with each other for performing several social activities. For example, an agent can require an information to another one, in the context of an activity of e-commerce, e-learning, e-government, e-health etc.

We denote by DS the set of devices and by AS the set of software agents. We also assume that the IoT devices belong to a *Network* N which, in turn, is composed of n different *Federated Networks* (F_i), where each federated network is managed by a dedicated device supported by an administrator agent (AA_i) which also locally manages the reputation system of the agents temporary running on its administrated domain.

We represent the relationships among the agents of N by a graph $G = \langle V, E \rangle$ where V and E, in turn, respectively represent *i*) the set of vertices belonging to G (each vertex of V is associated with a single agent belonging to N) and *ii*) the set of oriented edges belonging to G (each edge is associated with a relationship existing between two agents, as graphically depicted in Figure 1).

Within each federated network F_i, each agent can join with some agent sub-structures, called *teams*, built on the basis of the reputation values of the agents.

Example of teams are agents that want to cooperate for reaching a common goal as, for instance, grouping some people interested to participate to a guided visit to a museum.

We denote as g_j^i the j-th team g formed inside to the federated network F_i. We highlight that agents are free to change their affiliation with a federated network by moving from one to another one and, similarly, are free of joining with a team active on their current federated network. We also assume that each agent administrator is able to manage the teams active on its federated network: it can try to join with a team those agents having reputation values adequate for that team or, symmetrically, removing from a team agents having inadequate reputation values.

The honesty of an agent will be witnessed by its reputation value, which is represented by a real number obtained by observing the interactions of the agent with the other agents belonging to N when they perform Characterizing Interactions, i.e. those interactions that might characterize correct and incorrect behaviors, as we will describe in details below.

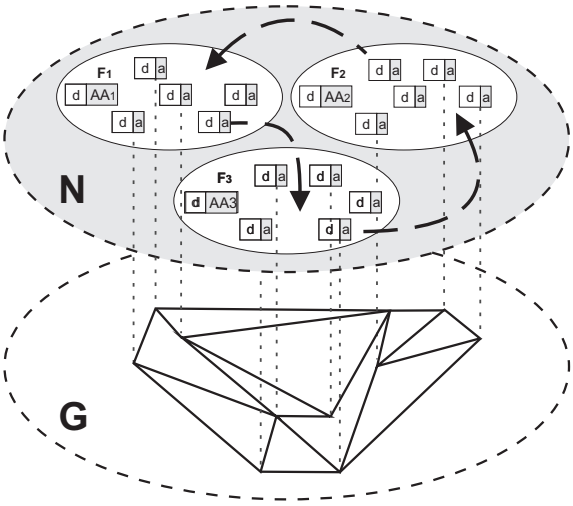

Fig. 1. The IoT Framework (N) with the federated networks (F) and the relationships graph (G)

IV. The Reputation Model

The Reputation of an agent is modeled as a real positive number $RV \in [0, 1]$ where a value close to 1 represents a good reputation.

Each newcomer agent receives an initial reputation that is not particularly penalizing for the newcomer, but it is adequate to discourage whitewashing strategies, which are taken by fraudulent agents that try to come back into the system to obtain a new immaculate positive reputation [62].

In particular, after any consumer agent y benefits from a service s, having a cost c, provided by an agent x, then both x and y will leave a feedback $feed$ (a real value belonging to the domain $[0, 1]$) to their counterpart. Then, the Relevance (ρ) of the required service s is defined as:

$$\rho = \begin{cases} \dfrac{c}{C} & \text{if } c < C \\ 1 & \text{otherwise} \end{cases} \tag{1}$$

where C is a cost threshold for an interaction (fixed by taking into account the context) after which the relevance of s is considered as saturated.

To hinder the advantages deriving to the agents carrying out systemic alternate behaviors, which consist of gaining reputation on interactions having a low relevance for spending it by cheating with those interactions having a high relevance, we assumed that not all the agent interactions can contribute in forming the reputation score of an agent. In other words we consider only those interactions, named Characterizing Interactions (CI), that mainly characterize and qualify the behavior of an agent, while we exclude those interactions giving to malicious agents the possibility of taking advantage from alternate behaviors to increase their reputation. We highlight that the introduction of CIs is devoted to quickly identifying the malicious agents.

More in detail, CIs are defined on the basis of their relevance and the received feedback. The ratio underlying a CI is that of considering: *i*) all the interactions receiving a low feedback independently from their relevance, i.e. the value of ρ and *ii*) all the interactions receiving a feedback having a value equal or greater than 0.5 but only if the value of this feedback $feed$ is lower then the relevance ρ of the service. In other words, the interactions that are excluded are all those receiving a positive feedback and for which benefits (i.e., feedback) are greater than costs (i.e., relevance). More formally, an interaction is characterizing when ρ and $feed$ assume the following values:

$$\begin{cases} feed < 0.5, \ \rho \in [0, 1] \\ feed \geq 0.5 \ \wedge \ \rho \geq feed \end{cases} \tag{2}$$

In Figure 2, in terms of ρ and $feed$, CIs are graphically described. More precisely, in this figure the white area is the region of the space ρ-$feed$ in which an interaction is assumed to be *characterizing*.

In our model, the reputation value of an agent k is updated by considering the latest occurred CIs. More formally, the reputation (RV) of the agent a_j is updated by considering the feedback given by the later h agents carried out CIs as follows:

$$RV_j = \sum_{i=1}^{h} \alpha_i \cdot \gamma_{j,i} \cdot \rho_{j,i}^{\frac{1}{i}} \cdot feed_{j,i}$$

where :

- α (Age) weights CIs so that the more recent an interaction is, more it contributes to the reputation value.

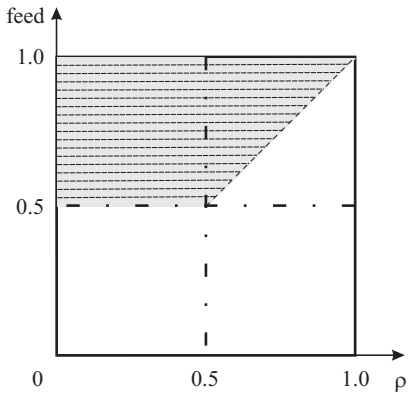

Fig. 2. Graphical representation of Characterizing Interactions. The white area is the region of the space ρ-$feed$ in which an interaction is assumed to be *characterizing*.

- γ (Reliability) limits the effects of those agents behaviors aimed to gain undue advantages by giving negative feedback in a systematic way. We denote the number of negative feedback of an agent and the overall number of the interactions carried out by NEG and TOT, respectively. Then γ is simply computed as the complement of the ratio $1 - \frac{NEG}{TOT}$, if $\frac{NEG}{TOT} > 0.5$, while it is set to 1 if $\frac{NEG}{TOT} \leq 0.5$. Note that the choice of the threshold 0.5 is devoted to define the maximum percentage of negative feedback to consider the reliability as saturated to 1.

V. Experimental design

To test the effectiveness of the proposed framework, we carried out an experimental campaign on a simulated scenario: section V-A describes the details of the team formation simulation, section V-B presents the reputation models we compared with our proposal, section V-C reports the simulation settings and, finally, results are exposed in section VI.

A. Simulation of Team Formation

We designed a team formation algorithm which is capable to drive team formation of IoT devices (i.e., agents) on the basis of their reputation scores (RV). To highlight as our framework, along with the team formation algorithm can lead to the growth of individual and global reputation within a federated network F, in the following we suppose that agents hold identical interests and preferences (see Section II). Moreover, we will assume that each consumer will pay a fee to the provider for a service only when they belong to different teams.

The team formation algorithm used to perform our experimental campaign is represented by the pseudocode listed in Algorithm 1. For each federated network F_i its administrator AA_i establish the maximum number of teams allowed in its managed domain and, for each of them, it sets also a suitable threshold $Gamma$ which is the minimum reputation value that is required to an agent for joining with that specific team. Consequently, within the federated network F, each agent will be affiliated with the team which "best fits" its RV. Periodically, the AA verifies whether the RV values of the agents of its administrated network are compliant with their team affiliations (i.e., the threshold Γ of their teams).

Therefore, agents could be migrated from one team to another one as a consequence of such reputation checks carried out by their AA. Furthermore, it may happen that an agent, at a certain time, is removed from every team because its current RV value is lower than all the team affiliation thresholds. The reader may refer to Table I for the symbols used in this work.

TABLE I
Table of the main symbols

Symbol	Description
F	a Federated Network
AA	the Agent Administrator of a federated network
FA	set of agents affiliated with a federated network
FG	set of groups active on a federated network
ΔT	time threshold set by a federated network administrator
g	a group of agents
RV	reputation value for a given agent
Γ	RV threshold for joining a given team
τ_{RV}	timestamp of the last computation of RV
τ_Γ	timestamp of last computation of the threshold for belonging to a team g
t	current timestamp

Algorithm 1 consists of two parts. In the former, the AA will check, for each team active in its administrated federated network, whether the reputation values of the agents holds a fresh value with respect to the last update of the threshold of the teams (lines 1–5). In the second part of the Algorithm 1 (lines 6–14), the AA checks whether, for each team having a fresh threshold value, one or more agents do not satisfy the requirement for joining with that team. In this case, through a call to the function *join()*, *i*) the agent is removed from the team and *ii*) the agent is affiliated with the team best fitting with its RV.

B. Reputation Models Comparison

To test the performance of our reputation model, with respect to the ability in recognizing malicious agents, three competitors have been selected: *i*) eBay [36]; *ii*) the well known SPORAS [37]; *iii*) the recent reputation system presented

Algorithm 1 The procedure executed by each AA.

Input: $FA_m, FG_m, \tau_\Gamma, \tau_{RV}$;

1: **for all** $a_i \in F_m$ **do**
2: **if** $\tau_{RV} \geq \tau_\Gamma$ **then**
3: retrieve and store the updated value of RV_i
4: **end if**
5: **end for**
6: **for all** $g_k \in F_m$ **do**
7: **if** $(t - \tau_\Gamma^k \geq \Delta T)$ **then**
8: **for all** $a_i \in g_k$ **do**
9: **if** $(RV_i < \Gamma_k)$ **then**
10: *Join* (a_i, k, FA_m, FG_m)
11: **end if**
12: **end for**
13: **end if**
14: **end for**

Algorithm 2 The function *Join* (a_i, k, FA_m, FG_m).

1: **if** $RV_i < \Gamma_m$ **then**
2: Remove a_i from group g_k
3: **end if**
4: **for all** $g_j \in F_m$ **do**
5: **if** ($RC_i \geq \Gamma_j$) **then**
6: assign a_i to the group g_j
7: **end if**
8: **end for**

in [39], appositely conceived for IoT scenarios. These competitors have been chosen on the basis of *i*) their compatibility with our framework and have been implemented according to their descriptions, except not relevant changes necessary to make homogeneous the comparison and *ii*) because they represent different, possible approaches to the problem.

More in detail, eBay is a well known centralized, feedback-based reputation system. The mechanism underlying eBay is very basic [63] and the reputation is the simple percentage of the only positive feedback with respect to their overall number received in a large time. Multiple feedback coming from the same counterpart are admitted only if they are not closed in time, while neutral feedback are not included in the calculation. To contrast multiple identities eBay, as SPORAS, assumes that when the system starts the agents (or newcoming agents) have assigned a null reputation. The eBay system has been extensively investigated and if, on the one hand, its simplicity has favored its adoption, on the other hand, it is exposed to malicious, and in particular collusive, behaviors.

Notwithstanding its age, SPORAS is still used for comparisons given its effectiveness [64]. The reputation of SPORAS ranges in $[0, 3000] \in \mathbb{R}$, as described in [37]. The ratio of SPORAS is to penalize low reputed agents by saving (usually) agents having a high reputation. The reputation updating is computed as:

$$R_i = R_{i-1} + \frac{1}{\theta} \cdot \Phi(R_{i-1}) R_i^{other}(W_i - E_i)$$
$$\Phi(R_{i-1}) = 1 - \frac{1}{1 + e^{-(R_{i-1} - D)\sigma}} \qquad E_i = R_{i-1}/D$$

where R_i and R_{i-1} are respectively the new and the current reputation, R_i^{other} is the reputation of who released the feedback W_i, θ is the number of ratings exploited in updating R_i, while σ is a parameter empirically set to 0.11.

The reputation model described in [39] has been designed to estimate the trustworthiness of Cloud Computing (CC) providers in an IoT context. In building the reputation, the effects due to unfaithful feedback ratings are mitigated by the use of the *credibility* and *certainty* weights. The first one is effective against collusive attacks, the other one hinders those activities based on false identities. Let $L_S(\Delta_{t_k})$ be a first reputation score (named *Local Objective Reputation*) referred to a service S made available by a CC provider and continuously computed on the basis of the received feedback F within a time windows Δ_{t_k} and weighted by credibility (Γ) and certainty (Λ) as:

$$L_S(\Delta_{t_k}) = F(\Delta_{t_k}) \cdot \Gamma(\Delta_{t_k}) \cdot \Lambda(\Gamma(\Delta_{t_k})$$

Then a *Global Objective Reputation* ($G_S(\Delta_{t_z})$ for z consecutive time windows is computed for each CC provider by adding all the *Local Objective Reputation* received in z, for a given service S, as:

$$G_S(\Delta_{t_z}) = \sum_{k=1}^{z} (L_S(\Delta_{t_k} \cdot \upsilon_k)$$

where $\upsilon_k \in [0.1] \in \mathbb{R}$ takes into account that older is the knowledge lower is its relevance. The reader can refer to [39] for a comprehensive description of how to calculate the Γ, Λ and υ weights. Finally, $G_S(\Delta_{t_z})$ is normalized in $[0, 1]$.

To make comparable the results given by this reputation model, we substituted the time window with a number of interactions, while with respect to the initial reputation of agents any information is provided in [39] about it and, therefore, we assumed to assign an initial reputation of 0.5 at all the agents likely our reputation model.

These reputation systems have been tested by adopting the setting described in V-C. However, against collusive behaviors any of these competitors in computing their reputation scores consider the interaction value which, together to the team formation, is fundamental in realizing the competitive scenario characterizing our framework.

C. Simulation Setting

We aimed at validating the presented approach on a few different aspects:

- a comparison between the performance of our reputation model and those of the reputation models, presented in V-B (Note as in this case our reputation model has been tested without to implement the agent teams in order to compare all systems on equal terms);
- the resilience of our framework in identifying dishonest actors which realize different and simultaneous typologies of attacks (see Section IV);
- how devices (i.e., agents) are distributed among the different teams based on their reputation value RV;
- how the RV increases with the number of interactions performed;
- the costs sustained (or, symmetrically, the gains obtained) by devices for services.

Simulations are involved only one federated network $F \in N$, where a sequence of interactions were performed by IoT devices, each one associated with its software agent. Furthermore, a percentage of cheater devices (i.e., agents) performing collusive, complainer and different modalities of alternate behaviors have been included into the simulations.

The setting adopted for the main parameters of these simulations is listed below:

- Two populations of 10^3 IoT devices/agents active in F, the first one of consumer agents and the other one of

TABLE II
EXPERIMENTAL PARAMETERS AND PARAMETERS OF THE FOR REPUTATION SYSTEMS: A) RESIOT; B) THE REPUTATION MODEL OF [39]; C) SPORAS; D) EBAY. (THE HORIZON h IS 4, 7 OR 10).

Description	Value/Range
Simulation Setting	
Consumer IoT device agents	10^3
Producer IoT device agents	10^3
Percentage of malicious	5, 15, 25
Simulation epochs	10^2
Interation for epoch	10^3
Alternate behavior ratios	randomly, $1:h$, $1:h/2$, $1:1$
Collusive behavior ratios	randomly, $1:h$, $1:h/2$, $1:1$
Complainers behavior ratios	randomly, $1:h$, $1:h/2$, $1:1$
Parameter Setting of System A	
Reputation range	$[0.0, 1.0]$
Initial reputation score	0.5
Service cost range	1.5 \$
Cost threshold	1 \$
Horizon (h)	4, 7, 10
Parameter Setting of System B	
Reputation range	$[0.0, 1.0]$
Initial RV score	0.5
Δ_t ($\Delta_t \equiv h$)	4, 7, 10
ψ_{S_i}	1
μ	0.6
z	4
Parameter Setting of System C	
Reputation range	$[0.0, 1.0]$
Initial reputation score	0
Horizon	none
Parameter Setting of System D	
Reputation range	$[0.0, 3000.0]$
Reputation range normalized	$[0.0, 1.0]$
Initial reputation score	0
σ	0.11
θ ($\theta_t \equiv h$)	4, 7, 10

provider agents[1].

- For each interaction a consumer and a provider agent were chosen in a random way from their respective communities. Interactions were arranged in epochs, each one consisting of 10^3 interactions so that, in average, each agent acted as consumer and provider at least one time for epoch.
- Simulations were carried out for 100 epochs, although only few epochs are necessary to obtain "stable" results.
- For our reputation model, an initial RV score set to 1.0 was assigned to each device (such a RV value was chosen on the basis of different issues), while for eBay and SPORAS the initial device reputation was set to 0 and to 0.5 for the other two systems.
- A cost $c_s \in [1, 1.5]$ was randomly assigned to each service s, while to define the relevance of s the cost threshold C was set to 1. This parameter is meaningful only for our reputation model.
- The number of interactions (i.e., the *horizon* h for our model or the time window Δ_t for [39]) used for the simulations varied from $h = 4$ to $h = 10$ with step 3.

[1]Note as in the most common scenarios there are many more consumers than producers, although other scenarios where consumers and providers have a similar numerosity exist. However, this later scenario is the most suitable for testing the resilience of a reputation system for the presence of more actors and, consequently, of more cheaters active into the system.

- Three different types of malicious behaviors have been taken into account and, depending on the different strategies, characterizing the interactions, implemented by honest and malicious devices, have occurred with different rates, respectively, randomly, $1:h$, $1:h/2$ and $1:1$ for all reputation systems with respect to the following malicious behaviors:
  - alternate - where low value interactions are correctly performed with the aim of improving the RV score for then spending it for cheating on high value interactions.
  - collusive - where two or more devices repetitively, mutually interact (usually on low value interactions) to grow their RV scores.
  - complainer - where, in a systemic way, negative feedback are given to damage the counterpart and, indirectly, gaining an undue advantage.
- To test our framework, the number of simulated teams was set to 3, while their affiliation RV thresholds were respectively set to 2.5, 4.5 and 6.0.

The reader may refer to Table II for the simulation environment and the parameters of the tested reputation system.

The simulations of our framework have been carried out on a IoT simulator based on the ACOSO methodology and platform (able to simulate IoT networks including IoT devices as well as to build real IoT systems) [2], [8]. This choice has allowed to achieve greater versatility in the development phase and greater efficiency in the execution of experiments and the processing of results (also) in real time.

VI. EXPERIMENTAL RESULTS

Here we discuss the experimental results obtained in the experimental campaign.

A. Reputation Models Comparison

The basic ability required to a reputation system is that of identifying the device nature (i.e. honest or malicious) and, to this aim, the first experiment compared the performance of our reputation model with those of the other systems described in section V-B.

All the reputation models have been tested for horizons $h = 4, 7, 10$ and malicious percentages $mal = 5, 15, 25\%$. The obtained results are shown in Table III and represented in Figure 3. In particular the labels A, B, C and D represent, respectively, the reputation model adopted in ResIoT, the reputation model presented in [39], SPORAS and eBay. We highlight that the ResIoT reputation model has been tested without simulating the presence of teams to make it completely comparable with the other proposals and, therefore, it does not perform at the best and its results are a bit worst than those presented in section VI-B.

The results of this experiment show that the ResIoT reputation model performs better than its competitors.

First of all, we can observe, by Figure 3, that our reputation system is more resilient than the other systems to the percentage of malicious active into the population. This result is clear

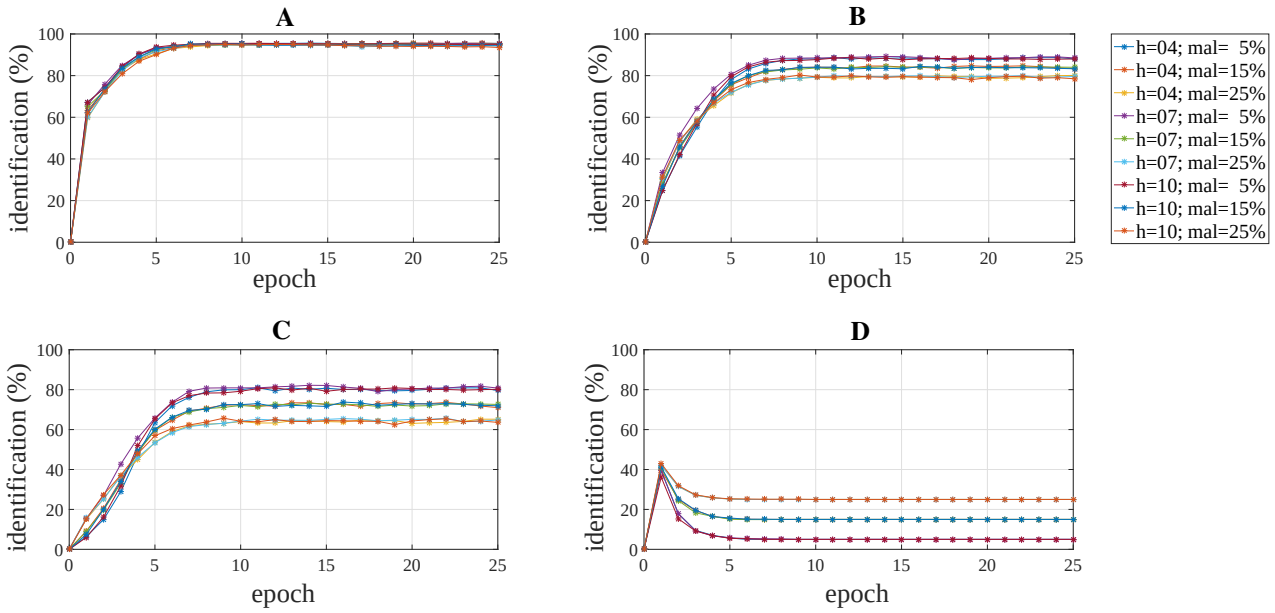

Fig. 3. Comparison among different reputation models in identifying honest and malicious for horizon $h = 4, 7, 10$ and malicious $mal = 5, 15, 25\%$ for reputation systems: A) ResIoT; B) the reputation model of [39]; C) SPORAS; D) eBay

TABLE III
COMPARISON AMONG DIFFERENT REPUTATION MODELS IN IDENTIFYING HONEST AND MALICIOUS FOR HORIZON $h = 4, 7, 10$ AND MALICIOUS $mal = 5, 15, 25\%$ FOR REPUTATION SYSTEMS: A) RESIOT; B) THE REPUTATION MODEL OF [39]; C) SPORAS; D) EBAY.

	horizon/malicious (%)								
h/mal (%)	4/5	4/15	4/25	7/5	7/15	7/25	10/5	10/15	10/25
epochs	System A								
1	67.2	62.3	59.7	66.0	65.1	60.0	67.3	62.3	61.9
5	92.9	91.9	90.5	93.4	92.3	91.5	93.7	92.9	90.1
10	95.3	95.4	94.6	95.2	95.0	94.7	95.5	95.2	94.7
15	95.5	95.3	95.0	95.1	95.0	94.6	95.2	94.7	94.7
20	95.0	95.6	94.5	95.5	95.2	94.4	95.1	94.6	94.0
25	95.5	95.4	95.1	95.3	95.1	94.5	95.0	94.3	93.5
epochs	System B								
1	24.9	27.7	30.2	33.4	28.5	30.7	24.7	26.9	31.4
5	78.1	75.6	71.7	80.7	75.8	72.0	79.5	76.3	73.3
10	95.3	95.4	94.6	95.2	95.0	94.7	95.5	95.2	94.7
15	88.0	84.1	79.2	88.5	83.7	79.3	87.7	84.0	79.3
20	87.7	84.4	79.2	88.5	83.7	79.3	88.3	84.0	79.0
25	88.0	83.3	80.1	88.5	84.0	79.6	88.0	83.3	78.5
epochs	System C								
1	6.4	9.1	15.1	15.4	9.0	15.8	6.0	7.5	15.3
5	63.5	59.6	53.6	65.8	59.7	53.4	65.3	60.2	56.9
10	80.0	72.5	64.0	80.9	72.1	64.2	79.2	72.5	64.2
15	80.7	72.6	64.0	80.9	72.1	64.2	79.2	71.6	64.5
20	79.6	72.8	63.1	80.3	71.8	65.1	80.6	73.0	64.3
25	79.6	71.0	65.2	80.8	72.6	64.8	80.2	71.9	63.6
epochs	System D								
1	39.5	39.7	42.1	39.5	41.0	42.1	36.2	41.3	43.0
5	5.7	15.4	25.2	5.8	15.1	25.2	5.5	15.7	25.3
10	5.0	15.0	25.0	5.0	15.0	25.0	5.0	15.0	25.0
15	5.0	15.0	25.0	5.0	15.0	25.0	5.0	15.0	25.0
20	5.0	15.0	25.0	5.0	15.0	25.0	5.0	15.0	25.0
25	5.0	15.0	25.0	5.0	15.0	25.0	5.0	15.0	25.0

for cases B, C and D where results are grouped based on the considered percentage of malicious devices. In particular, we draw the following observations and analysis:

- case B ([39]): represents the best competitor of the ResIoT reputation model, it shows a good resilience against some of the attacks carried out in the tests. In particular it gives the same relevance to all the interactions; as a consequence, it is easier, for the malicious agents, to carry out collusive attacks. It is a good reputation model, which is able to work also with a limited number of behavioral data. The related performances are, however, lower then than 11% and, therefore the ResIoT reputation model

perform better than B.

- case C (SPORAS): it is considered, in the literature, a good reputation system. By the experimental results we observed as this system is not able to provide any useful differentiation, in terms of reputation score, between honest and malicious actors. Indeed, by stressing the system by simulating continuous attacks, SPORAS does not allow to recognize malicious actors providing all them with reputation scores high enough to be classified as honest. More specifically, we can observe that, at the 25-th epoch, less than 1% of malicious is identified and, therefore, we consider it as not resilient and useless for our purposes.
- case D (eBay reputation system) is the worst among the competitors. Indeed, from a practical point of view, the results are grouped based on the percentage of malicious considered in the simulations (i.e., 5%, 15% and 25%). At a first look, we can deduce that eBay is capable of recognizing all malicious (but none honest). Actually this system is defenseless against the most common malicious attacks and, as a consequence, all the reputation scores are very lower both for malicious that for honest devices. Therefore, it is not able to distinguish honest and malicious actors; moreover, it does not perform as the ResIoT reputation model.

In the light of the discussed results, we argue that the tested competitors performed worst of our proposal also in the other experiments. In particular, we remark that the ResIoT reputation model outperforms that described in [39] (case B), which is a very recent and effective reputation model. Indeed, the ResIoT reputation model takes a significant benefit from the adoption of different relevance among the interactions on the basis of their value, also introducing the CIs.

B. Malicious detection

The experimental results described here represent the ability of our framework in recognizing the nature (i.e., honest or malicious) of consumer and provider devices/agents, on the basis of their RV by implementing also the agent teams, differently from the previous experiment. In this case we produced results for several different scenarios characterized by different values of horizon, from $h = 4$ to $h = 10$ with step 3 and the percentage (with respect the overall device/agent population) of malicious agents from 5% to 25%, with step 10%.

The obtained results are shown in Table IV and represented in Figure 4. We observe that results are better than those presented in Section VI-A, because in the previous results the presence of teams have been considered to make our reputation model more comparable with its competitors.

These new results show that the nature of actors is quickly recognized with a high precision $> 95\%$ in $6 \div 10$ epochs. After the 10-th epoch all the honest actors are totally recognized, while false positive for malicious varied from 2% to 9% based on the overall percentage of malicious with respect to consumer and provider population. Moreover, around the 45-th epoch the maximum error is less than the 2.5%, while little fluctuations tightly depend on the alternate, endless attacks periodically carried out by malicious agents by adopting different modalities.

In order to verify the sensitivity of our model in recognizing honest and malicious when the presence of cheaters increases, we tested our framework also with percentage of malicious varying from 0% to 100%, with step 5% of the overall device population for the horizons $h = 4$ and $h = 10$. The results are reported in Figure 5 at the 50-th epoch and show as, from a practical viewpoint, the framework performance starts to decreases when the percentage of malicious is more than the 25% (for both the considered horizons, i.e., $h = 4$ and $h = 10$), which is already a not realistic threshold in real systems. After this value the results obtained in recognizing the actors progressively worsen for then improving, also because the majority of devices has became malicious. Moreover, trivially the framework is more resilient for $h = 10$ than for $h = 4$.

C. Team affiliation

In a third experiment we investigated on the affiliation of devices among the teams active in F, on the basis of their RV. Figure 6 shows the results w.r.t the horizon thresholds $h = 4, 7, 10$ and a percentage of malicious devices equal to the $5, 15, 25\%$ of the whole population. In this experiment, and for all the scenarios, we adopted the affiliation RV thresholds reported in Section V-C.

From the result analysis we highlight that:

- almost all the scenarios correctly work except with a very small horizon (e.g., $h = 4$) and a very large percentage of malicious (e.g., 25% of the population) and almost all of them are not joined with any team because their RV score is too lower for a team affiliation, this result becomes stable in less than 10 epochs;
- a low horizon does not allow the affiliation with the team 3 because it is very difficult to reach a RV score equal or greater ot the affiliation threshold adopted for this team (see Section VI) and maintains it over time;
- a large horizon allows to the most part of the honest devices to gain a RV score adequate to belong all them to the team 3;
- the adopted affiliation thresholds obviously affect the distribution trend above discussed.

D. RV

The behavior of the RV when the percentage of cheaters and the horizon vary has been investigated in this experiment. Results are always referred to horizon thresholds $h = 4, 7, 10$ and percentage of malicious devices of $5, 15, 25\%$ of the population. The results presented in Figure 7 confirmed the relationship existing among RV and horizon and numerosity of malicious devices, already evident in the previous experiments.

E. Economic benefits

This set of experiments deals with the economic implications of our framework computed at the 25-th epoch, this

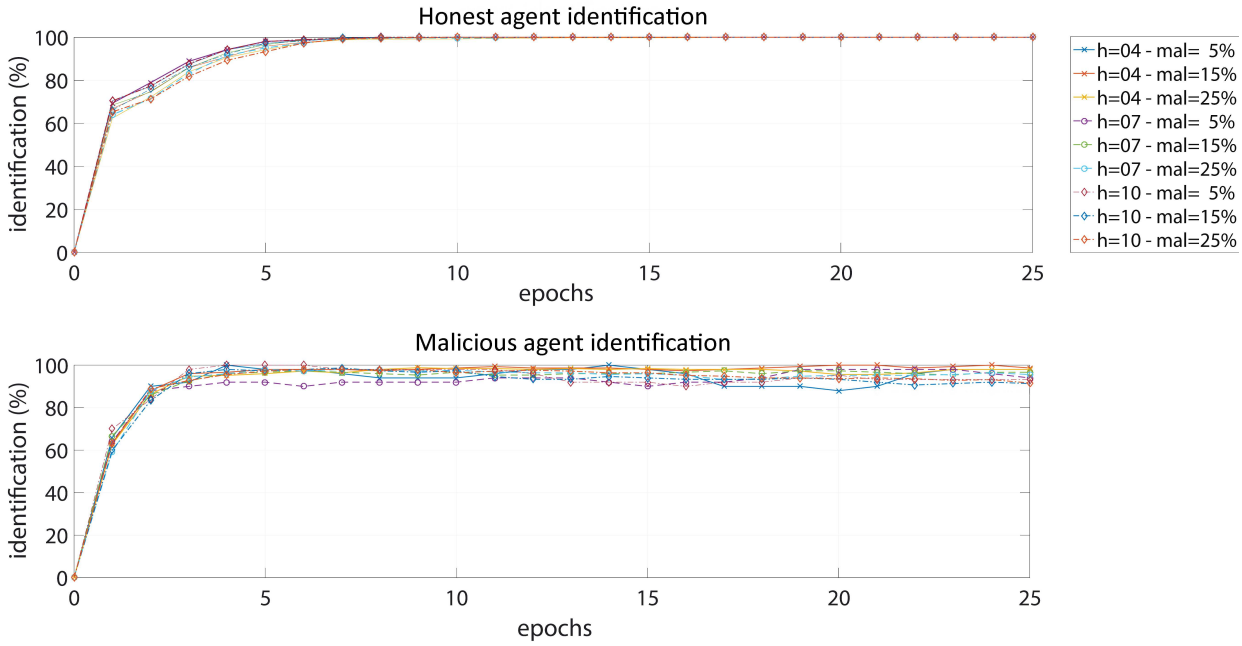

Fig. 4. Honest and malicious agent identification for horizon $h = 4, 7, 10$ and malicious $mal = 5, 15, 25\%$.

TABLE IV
HONEST AND MALICIOUS AGENT IDENTIFICATION FOR HORIZON $h = 4, 7, 10$ AND MALICIOUS $mal = 5, 15, 25\%$.

	horizon/malicious (%)								
h/mal (%)	4/5	4/15	4/25	7/5	7/15	7/25	10/5	10/15	10/25
epochs	Honest								
1	70.5	66.8	62.4	69.4	68.5	64.0	7.4	66.1	65.3
5	97.2	95.9	94.3	98.1	96.6	95.1	98.0	97.2	93.3
10	100.0	100.0	99.7	100.0	100.0	100.0	100.0	100.0	100.0
15	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0
20	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0
25	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0
epochs	Malicious								
1	66.0	63.3	62.8	64.0	66.7	59.2	70.0	60.0	63.2
5	98.0	98.0	96.0	92.0	96.7	98.0	100.0	97.3	97.2
10	94.0	98.7	98.4	92.0	96.7	97.6	98.0	97.3	96.4
15	98.0	98.0	98.4	90.0	96.0	96.0	92.0	94.0	96.4
20	88.1	100.0	95.6	98.0	97.3	95.2	90.0	93.3	93.6
25	98.0	98.7	98.0	94.1	96.7	95.6	88.0	91.3	91.6

means that each consumer (i.e., provider) performed 25 interactions in average. In Figures 8 are shown the results in terms of economic benefits, i.e. the saved money, which vary from 4.74 $ to 3.67 $ depending it from both the horizon and the percentage of malicious devices considered in the simulations. Such results represent the evidence that there are not economic benefits, neither on a short time, for devices acting not correctly or, in other words, honest devices both spent less (or, symmetrically, providers gain more) for services than malicious one.

VII. FINAL DISCUSSION AND CONCLUSIONS

The ResIoT framework has been conceived to support the formation of social teams of IoT devices associated with agents, provided of resilience against possible malicious activities.

In our proposal, this purpose is pursued using an agent reputation model taking into accounts the feedback provided by the agents themselves during their activities. In this model, the overall reputation value of each agent team is updated in time implementing some suitable countermeasures to avoid collusive and some misleading activities finalized to gain incorrect reputation values. Moreover, in updating the reputation only the feedback related to those interactions satisfying some requirements are considered. An apposite team formation algorithm that exploits the reputation values of the agents has been introduced to support the formation of a competitive scenario. In particular, if an agent wants to join with a group having a high average reputation, it must obtain a high individual reputation value.

A. Advantages of the approach

The experimental results shown in Section VI highlights that ResIoT is highly resilient to malicious activities, that

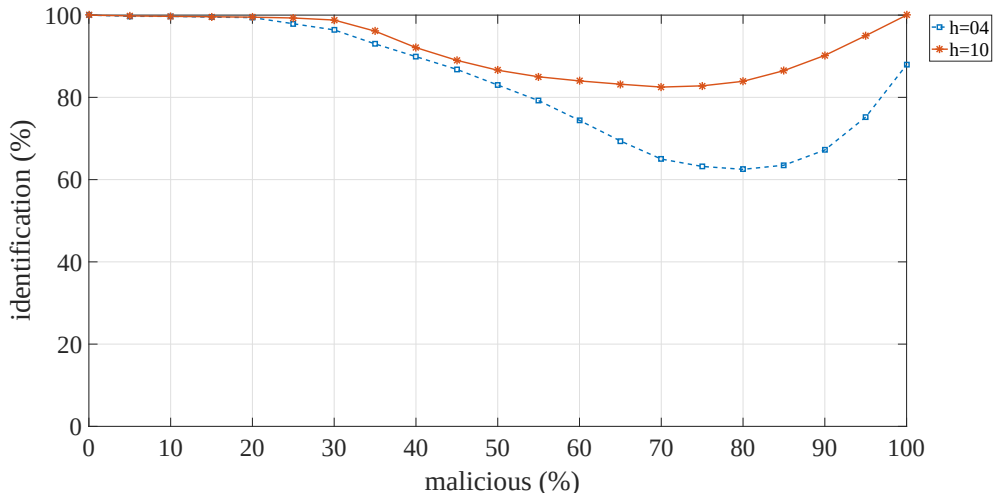

Fig. 5. Sensitivity for $h = 4$ and $h = 10$ at the 50-th epoch in identifying the honest and malicious nature when the malicious percentage increases into the population

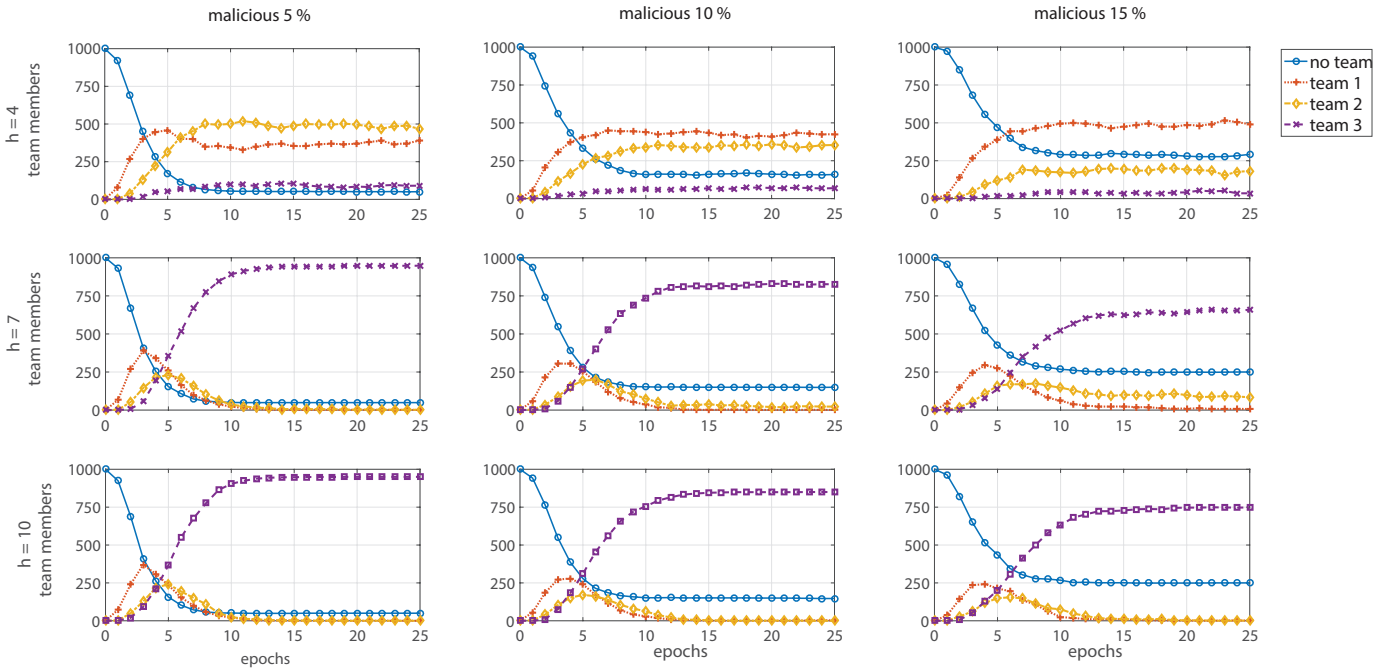

Fig. 6. Team member affiliation for horizon $h = 5, 7, 10$ and a percentage of malicious $mal = 5, 15, 25\%$ of the overall population.

are quickly detected if the number of malicious agents is below a certain threshold. In particular, the experiments have shown that the combined use of the reputation model and the group formation algorithm allows the framework to effectively and efficiently working for guaranteeing the system resilience. Moreover, ResIoT shows the relevant advantage of allowing IoT objects to migrate across different federated administrative environments by carrying their reputation scores and allowing, through the presence of the teams, the possibility to select reliable partners.

B. Forthcoming researches and current limitations

The results of the test that we carried out highlighted some issues that involve different aspects of the proposed framework which deserve to be investigated in our forthcoming researches. In particular, the team formation process is currently based on a few preliminary tests carried out by adopting a trial and error modality. We observed that this way of forming groups and setting the affiliation thresholds lacks versatility and efficiency in following possible changes occurring into the environment (e.g. an increase of the device/agent population or of the percentage of malicious actors). Therefore, we are studying an effective mechanism able to dynamically and automatically optimize the number of teams and their reputation affiliation thresholds in accord with evolving scenarios. Moreover, the good results obtained in validating our approach but only on the basis of some (realistic) simulations, suggest us another priority in our ongoing researches. Therefore, in

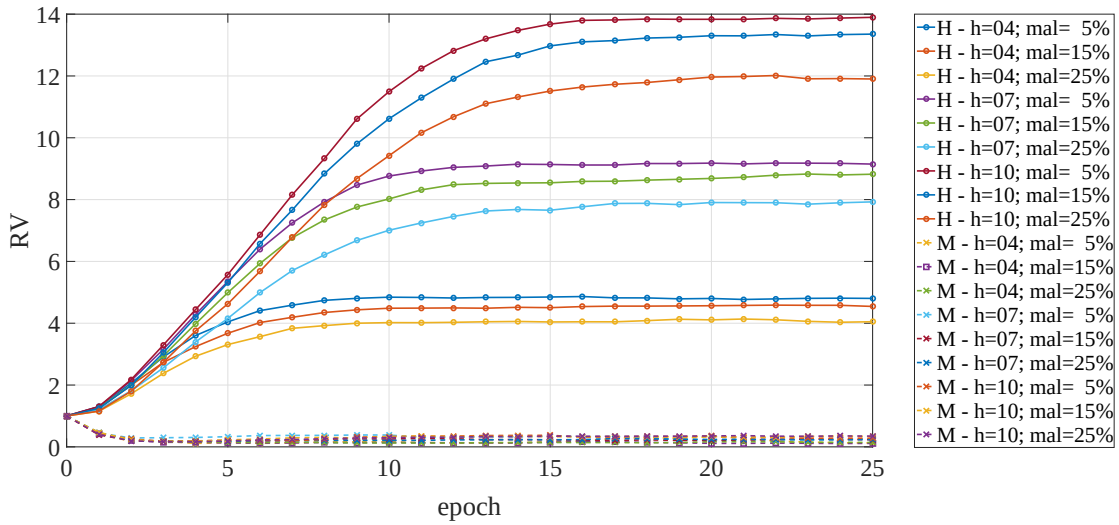

Fig. 7. RV for honest (H) and malicious (M) devices for horizon $h = 5, 7, 10$ and a percentage of malicious $mal = 5, 15, 25\%$ of the overall population.

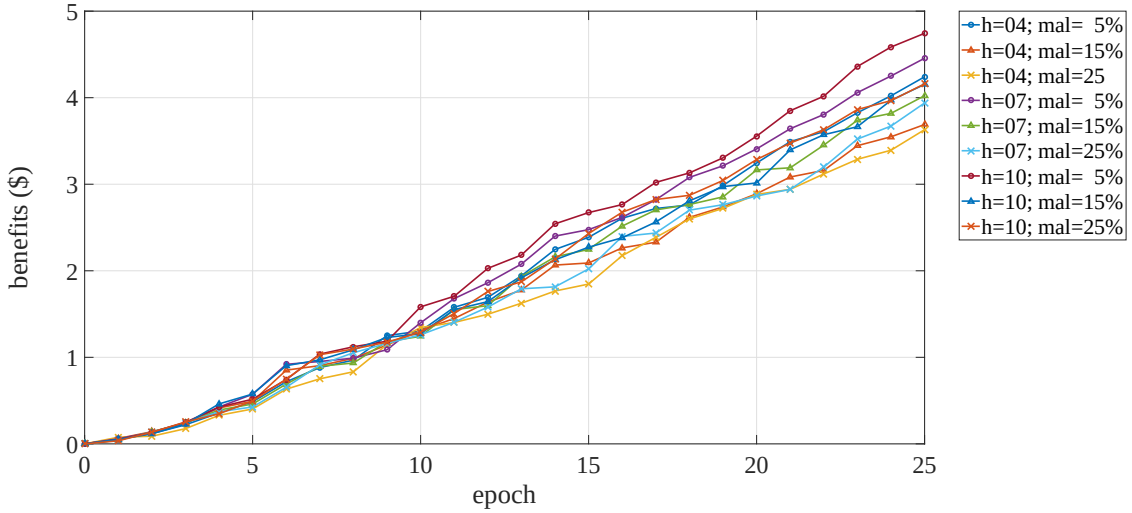

Fig. 8. profit of honest and malicious consumers at the 25-th epoch for $h = 5, 7, 10$ and a percentage of malicious $mal = 5, 15, 25\%$ of the overall population.

order to obtain a confirm about the advantages described above, there is the need to carry out an experimental campaign in a real IoT scenario, although the implementation of teams requires the availability of a considerable number of IoT devices. To overcome such constraint, currently we are designing an experiment by exploiting both real and simulated IoT devices in a vehicle-to vehicle (V2V) context aimed to provide/consume services (i.e., traffic information). Obviously, a real scenario will require also to solve other problems that we have not considered in this contribution like those deriving from overloading or unbalanced communication occurring among the different actors (i.e., consumers and providers).

Finally, the effectiveness demonstrated by the reputation system shows that also that different IoT, as well as non-IoT, contexts could benefit from the adoption of the reputation model proposed in this paper. Indeed, competitive scenarios, where it is possible to assign a value (real or also virtual) to the interactions represent possible opportunities to apply our reputation model also without to implement the teams, as witnessed by the experimental results presented into the in Section VI-A. However, a great attention should be given in defining a "good" CI, which appears to be context-sensitive and represents an essential component for allowing to our reputation model to work with a very limited number of behavioral observations that, in our opinion, is one of its most important peculiarity.

As future work the proposed algorithm's parameters will be optimized with the advanced approaches, e.g., [65], [66], [67].

ACKNOWLEDGMENTS

This work has been partially supported by the University of Catania, Piano per la Ricerca 2016-2018 - Linea di intervento

1 (Chance), prot. 2019-UNCTCLE-0343614.

REFERENCES

[1] K. Ashton, "That' internet of things' thing. rfid journal, june," 2009.

[2] G. Fortino, W. Russo, C. Savaglio, W. Shen, and M. Zhou, "Agent-oriented cooperative smart objects: From iot system design to implementation," IEEE Transactions on Systems, Man, and Cybernetics: Systems - in press (2018). DOI:10.1109TSMC.2017.2780618, 2018.

[3] M. Barcelo, A. Correa, J. Llorca, A. M. Tulino, J. L. Vicario, and A. Morell, "Iot-cloud service optimization in next generation smart environments," IEEE Journal on Selected Areas in Communications, vol. 34, no. 12, pp. 4077–4090, 2016.

[4] G. Fortino, F. Messina, D. Rosaci, and G. M. L. Sarné, "Using trust and local reputation for group formation in the cloud of things," Future Generation Computer Systems, vol. 89, pp. 804–815, 2018.

[5] G. Kortuem, F. Kawsar, V. Sundramoorthy, and D. Fitton, "Smart objects as building blocks for the internet of things," IEEE Internet Computing, vol. 14, no. 1, pp. 44–51, 2010.

[6] Y. Kim, S. Lee, and I. Chong, "Orchestration in distributed web-of-objects for creation of user-centered iot service capability," Wireless personal communications, vol. 78, no. 4, pp. 1965–1980, 2014.

[7] Z. Wen, R. Yang, P. Garraghan, T. Lin, J. Xu, and M. Rovatsos, "Fog orchestration for internet of things services," IEEE Internet Computing, vol. 21, no. 2, pp. 16–24, 2017.

[8] G. Fortino, R. Gravina, W. Russo, and C. Savaglio, "Modeling and simulating internet-of-things systems: A hybrid agent-oriented approach," Computing in Science & Engineering, vol. 19, no. 5, pp. 68–76, 2017.

[9] D. Calvaresi, M. Marinoni, A. Sturm, M. Schumacher, and G. Buttazzo, "The challenge of real-time multi-agent systems for enabling iot and cps," in Proceedings of the international conference on web intelligence. ACM, 2017, pp. 356–364.

[10] M. Hamzei and N. J. Navimipour, "Toward efficient service composition techniques in the internet of things," IEEE Internet of Things Journal, vol. 5, no. 5, pp. 3774–3787, 2018.

[11] B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, "Capability-based access control delegation model on the federated iot network," in The 15th International Symposium on Wireless Personal Multimedia Communications. IEEE, 2012, pp. 604–608.

[12] L. Cui, F. P. Tso, and W. Jia, "Federated service chaining: Architecture and challenges," IEEE Communications Magazine, vol. 58, no. 3, pp. 47–53, 2020.

[13] T. Leppänen, J. Riekki, M. Liu, E. Harjula, and T. Ojala, "Mobile agents-based smart objects for the internet of things," in Internet of Things Based on Smart Objects. Springer, 2014, pp. 29–48.

[14] H. Zhu and M. Zhou, "Role-based collaboration and its kernel mechanisms," IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 36, no. 4, pp. 578–589, 2006.

[15] P. De Meo, F. Messina, M. N. Postorino, D. Rosaci, and G. M. L. Sarné, "A reputation framework to share resources into iot-based environments," in 2017 IEEE 14th International Conference on Networking, Sensing and Control (ICNSC). IEEE, 2017, pp. 513–518.

[16] M. Roopa, S. Pattar, R. Buyya, K. R. Venugopal, S. Iyengar, and L. Patnaik, "Social internet of things (siot): Foundations, thrust areas, systematic review and future directions," Computer Communications, 2019.

[17] W. Li, J. Wu, Q. Zhang, K. Hu, and J. Li, "Trust-driven and qos demand clustering analysis based cloud workflow scheduling strategies," Cluster computing, vol. 17, no. 3, pp. 1013–1030, 2014.

[18] M. Trnka, J. Svacina, T. Cerny, E. Song, J. Hong, and M. Bures, "Securing internet of things devices using the network context," IEEE Transactions on Industrial Informatics, 2019.

[19] H. H. Chang and S.-S. Chuang, "Social capital and individual motivations on knowledge sharing: Participant involvement as a moderator," Information & management, vol. 48, no. 1, pp. 9–18, 2011.

[20] C.-M. Chiu, M.-H. Hsu, and E. T. Wang, "Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories," Decision support systems, vol. 42, no. 3, pp. 1872–1888, 2006.

[21] J. Doodson, J. Gavin, and R. Joiner, "Getting acquainted with groups and individuals: Information seeking, social uncertainty and social network sites," in 17th Int. AAAI Conf. on Weblogs and Social Media, 2013.

[22] J. M. Leimeister, P. Sidiras, and H. Krcmar, "Success factors of virtual communities from the perspective of members and operators: An empirical study," in System Sciences, 2004. Proc. of the 37th Annual Hawaii Int. Conf. on. IEEE, 2004, pp. 10–pp.

[23] H. Zhu, "Avoiding conflicts by group role assignment," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 46, no. 4, pp. 535–547, 2016.

[24] L. Fotia, F. Messina, D. Rosaci, and G. M. L. Sarné, "Using local trust for forming cohesive social structures in virtual communities," The Computer Journal, vol. 60, no. 11, pp. 1717–1727, 2017.

[25] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013.

[26] K. Benson, "Enabling resilience in the internet of things," in 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops). IEEE, 2015, pp. 230–232.

[27] M. Srivatsa, L. Xiong, and L. Liu, "Trustguard: countering vulnerabilities in reputation management for decentralized overlay networks," in Proc. 14th int. conf. on World Wide Web. ACM, 2005, pp. 422–431.

[28] Y. Ruan and A. Durresi, "A survey of trust management systems for online social communities–trust modeling, trust inference and attacks," Knowledge-Based Systems, vol. 106, pp. 150–163, 2016.

[29] M. Daudi, J. B. Hauge, and K.-D. Thoben, "A trust framework for agents? interactions in collaborative logistics," in Dynamics in Logistics. Springer, 2017, pp. 53–63.

[30] M. Aazam, I. Khan, A. A. Alsaffar, and E.-N. Huh, "Cloud of things: Integrating internet of things and cloud computing and the issues involved," in Applied Sciences and Technology (IBCAST), 2014 11th International Bhurban Conference on. IEEE, 2014, pp. 414–419.

[31] M. G. V. Kumar and U. Ragupathy, "A survey on current key issues and status in cryptography," in Wireless Communications, Signal Processing and Networking (WiSPNET), Int. Conf. on. IEEE, 2016, pp. 205–210.

[32] J. Fogel and E. Nehmad, "Internet social network communities: Risk taking, trust, and privacy concerns," Computers in Human Behavior, vol. 25, no. 1, pp. 153–160, 2009.

[33] L. Xiong and L. Liu, "Supporting reputation-based trust for peer-to-peer electronic communities," IEEE Transaction on Knowledge and Data Engineering, vol. 16, no. 7, pp. 843–857, 2004.

[34] D. Rosaci, G. M. Sarné, and S. Garruzzo, "Integrating trust measures in multiagent systems," International Journal of Intelligent Systems, vol. 27, no. 1, pp. 1–15, 2012.

[35] T. Huynh, N. Jennings, and N. Shadbolt, "An integrated trust and reputation model for open multi-agent system," Autonmous Agent and Multi Agent Systems, vol. 13, 2006.

[36] D. Houser and J. Wooders, "Reputation in auctions: Theory, and evidence from ebay," Journal of Economics & Management Strategy, vol. 15, no. 2, pp. 353–369, 2006.

[37] G. Zacharia, A. Moukas, and P. Maes, "Collaborative reputation mechanisms for electronic marketplaces," Decision support systems, vol. 29, no. 4, pp. 371–388, 2000.

[38] L. Tseng, Y. Wu, H. Pan, M. Aloqaily, and A. Boukerche, "Reliable broadcast in networks with trusted nodes," in 2019 IEEE Global Communications Conference (GLOBECOM). IEEE, 2019, pp. 1–6.

[39] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang, and D. Chen, "Enhancing cloud-based iot security through trustworthy cloud service: An integration of security and reputation approach," IEEE Access, vol. 7, pp. 9368–9383, 2019.

[40] S. Indiramma, , and Anandakumar, "Tcm: A trust computation model for collaborative decision making in multi-agent system," 2008.

[41] J. Sabater and C. Sierra, "Regret: reputation in gregarious societies," in Proc. of the 5th Int. Conference on Autonomous agents. ACM, 2001, pp. 194–195.

[42] S. A. Ghasempouri and B. T. Ladani, "Modeling trust and reputation systems in hostile environments," Future Generation Computer Systems, vol. 99, pp. 571–592, 2019.

[43] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," Computer networks, vol. 76, pp. 146–164, 2015.

[44] J. Guo, R. Chen, and J. J. Tsai, "A survey of trust computation models for service management in internet of things systems," Computer Communications, vol. 97, pp. 1–14, 2017.

[45] M. Aloqaily, S. Otoum, I. Al Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," Ad Hoc Networks, vol. 90, p. 101842, 2019.

[46] F. Bao and I.-R. Chen, "Dynamic trust management for internet of things applications," in Proc. of the 2012 int. work. on Self-aware internet of things. ACM, 2012, pp. 1–6.

[47] R. Chen, F. Bao, and J. Guo, "Trust-based service management for social internet of things systems," IEEE transactions on dependable and secure computing, vol. 13, no. 6, pp. 684–696, 2016.

[48] C. Vallati, E. Mingozzi, G. Tanganelli, N. Buonaccorsi, N. Valdambrini, N. Zonidis, B. Martínez, A. Mamelli, D. Sommacampagna, B. Anggorojati et al., "Betaas: A platform for development and execution of machine-to-machine applications in the internet of things," Wireless Personal Communications, vol. 87, no. 3, pp. 1071–1091, 2016.

[49] Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the internet of things: A context-aware and multi-service approach," Computers & Security, vol. 39, pp. 351–365, 2013.

[50] E. M. Schooler, D. Zage, J. Sedayao, H. Moustafa, A. Brown, and M. Ambrosin, "An architectural vision for a data-centric iot: Rethinking things, trust and clouds," in Distributed Computing Systems, 2017 IEEE 37th Int. Conf. on. IEEE, 2017, pp. 1717–1728.

[51] M. D. Alshehri, F. K. Hussain, and O. K. Hussain, "Clustering-driven intelligent trust management methodology for the internet of things (citm-iot)," Mobile Networks and Applications, pp. 1–13, 2018.

[52] J. P. Sterbenz, "Smart city and iot resilience, survivability, and disruption tolerance: Challenges, modelling, and a survey of research opportunities," in 2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM). IEEE, 2017, pp. 1–6.

[53] I. Al Ridhawi, S. Otoum, M. Aloqaily, Y. Jararweh, and T. Baker, "Providing secure and reliable communication for next generation networks in smart cities," Sustainable Cities and Society, vol. 56, p. 102080, 2020.

[54] H. Li, Q. Lu, and T. Huang, "Convergence analysis of a distributed optimization algorithm with a general unbalanced directed communication network," IEEE Transactions on Network Science and Engineering, vol. 6, no. 3, pp. 237–248, 2019.

[55] H. Sándor, B. Genge, and G. Sebestyén-Pál, "Resilience in the internet of things: The software defined networking approach," in 2015 IEEE International Conference on Intelligent Computer Communication and Processing (ICCP). IEEE, 2015, pp. 545–552.

[56] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in iot using blockchain," in MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM). IEEE, 2017, pp. 261–266.

[57] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A systematic literature review of blockchain cyber security," Digital Communications and Networks, 2019.

[58] L. Tseng, L. Wong, S. Otoum, M. Aloqaily, and J. B. Othman, "Blockchain for managing heterogeneous internet of things: a perspective architecture," IEEE Network, vol. 34, no. 1, pp. 16–23, 2020.

[59] Z. A. Khan, J. Ullrich, A. G. Voyiatzis, and P. Herrmann, "A trust-based resilient routing mechanism for the internet of things," in Proceedings of the 12th International Conference on Availability, Reliability and Security, ser. ARES '17. New York, NY, USA: ACM, 2017, pp. 27:1–27:6.

[60] H. Li, Q. Lu, and T. Huang, "Distributed projection subgradient algorithm over time-varying general unbalanced directed graphs," IEEE Transactions on Automatic Control, vol. 64, no. 3, pp. 1309–1316, 2019.

[61] L. Liu, M. Loper, Y. Ozkaya, A. Yasar, and E. Yigitoglu, "Machine to machine trust in the iot era." in TRUST@ AAMAS, 2016, pp. 18–29.

[62] M. Feldman, C. Papadimitriou, J. Chuang, and I. Stoica, "Free-riding and whitewashing in peer-to-peer systems," IEEE Journal on selected areas in communications, vol. 24, no. 5, pp. 1010–1019, 2006.

[63] http://www.ebay.com , "2008."

[64] A. J. Bidgoly and B. T. Ladani, "Benchmarking reputation systems: A quantitative verification approach," Computers in Human Behavior, vol. 57, pp. 274–291, 2016.

[65] P. Zhang, S. Shu, and M. Zhou, "An online fault detection model and strategies based on svm-grid in clouds," IEEE/CAA Journal of Automatica Sinica, vol. 5, no. 2, pp. 445–456, 2018.

[66] J. Wang and T. Kumbasar, "Parameter optimization of interval type-2 fuzzy neural networks based on pso and bbbc methods," IEEE/CAA Journal of Automatica Sinica, vol. 6, no. 1, pp. 247–257, 2019.

[67] S. Gao, M. Zhou, Y. Wang, J. Cheng, H. Yachi, and J. Wang, "Dendritic neuron model with effective learning algorithms for classification, approximation, and prediction," IEEE transactions on neural networks and learning systems, vol. 30, no. 2, pp. 601–614, 2018.