# A Reputation Agent Model for Reliable Vehicle-to-Vehicle Information

Giuseppe M. L. Sarné
Department DICEAM, University of Reggio Calabria, Loc. Feo di Vito, 89122 Reggio Cal., Italy, e-mail:sarne@unirc.it

***Abstract*—In the next future, an incredible amount of objects will be mutually interconnected to exchange information and services to realize more and more complex tasks. Unfortunately, this process places significant risks on the interconnected objects and their users, due to the adoption of unreliable information sources. Consequently, an emerging issue is of improving this aspect. In open and dynamic software agent contexts, this is a relevant question given the agents capability to quickly evaluate the potential effects of a greatest number of malicious behaviors in automated way. The adoption of authentication techniques is unable to assure the reliability of the information sources, differently from trust and reputation systems that fit well with such problems. The reliability of the information sources is becoming relevant also in the context of urban mobility where vehicles could acquire information coming not only from the infrastructures but also from other vehicles. Reliable information sources are fundamental to contribute in reducing the negative traffic effects in urban centers, which is among the most important factors affecting citizens' life quality. In the above scenario, we designed a distributed reputation model, working within an agent framework, to assure the reliability of the information sources in vehicle-to-vehicle interactions. In particular, the designed reputation model is able to detect malicious and cheating information sources as shown by some preliminary simulations carried out on a simple urban test network.**

***Index Terms*—Information source, Multiagent system, Reputation, Trust, Vehicle-to-Vehicle interactions**

## I. Introduction

In the next future, an incredible amount of objects provided with communication capabilities will cooperate by exchanging information and services to realize more and more complex and advanced computational tasks [1]. This pervasive process will modify manifold aspects of our lives by making available new opportunities in smart environments [2], [3].

To rule the increasing complexity of such environments, an efficient solution consists of associating software agents with the involved actors, independently on their nature of objects or humans. Unfortunately, this scenario presents significant risks in terms of low security and/or privacy as well as unreliable information and/or services due to malicious behaviors addressed to gain undue benefits [4]. Therefore, an emerging issue is that of improving the resilience towards malicious attacks in order to increase the level of confidence in all the involved participants. In presence of software agents this issue is of primary relevance given their capabilities to quickly evaluate the potential effects of a greatest number of malicious behaviors in automated way.

In general, in open smart environments the task of avoiding –or more correctly limiting– risks is not a trivial challenge, particularly when sensitive infrastructures and services are involved [5]. In fact, a potentially great number of interconnected entities, also equipped with autonomous intelligence, should both to recognize different threats and activate suitable countermeasures without affecting the system efficiency. Usual approaches are based on the adoption of cryptographic techniques. However, they are more effective in improving security and privacy while are ineffective with respect to many other threats. A useful contribution can arrive from trust and reputation systems [6], [7], which have widely shown their capabilities in many fields where cryptographic techniques are ineffective as, for instance, in estimating the reliability of an information source. This type of knowledge is particularly important in presence of open and dynamic environments which could encourage anomalous behaviors [8].

The reliability of the information sources is becoming relevant also in the context of urban mobility [9], [10]. Indeed, a wide number of architectures and models consider the problem of exchanging information not only between vehicles and the network infrastructures, but also among vehicles [11]. In Intelligent Transport Systems (ITS) scenarios, the availability of updated and reliable information is fundamental both for the transport network management and for allowing vehicles (i.e., the drivers) to adopt local best choices [12]. Such actions could limit the negative traffic effects, which is one among the most important factors affecting the citizens' life quality [13].

To solve the problem of the information source reliability, an *Agent-based Reputation System* (ARS) is proposed, where more typologies of intelligent software agents work together to manage reputation information on safe communications (it is supposed that at least a communication channel is available for realizing vehicle-to vehicle interactions) [14], [15]. Note that all the authentication tasks performed by the agents are considered as orthogonal issues with respect to the focus of identifying reliable sources and, therefore, in the following they will not be considered in detail.

In particular, ARS exploits four typologies of agents respectively named *Manager Agent* (MA), *Bridge Agent* (BA), *Vehicle Agent* (VA) and *Stub Agent* (SA) which will be described more in detail in the next section. The reputation about the reliability of an information source, (i.e., a Vehicle Agent) is spread within the system [16] by means of vehicle-to-vehicle interactions [17]. To this purpose, a reputation model, which includes some countermeasures addressed to identify quickly malicious behaviors, has been appositively conceived. A set of experiments simulating vehicles moving on a simple transport network [18], [19] tested the proposed agent system with interesting results.

The paper is organized as follows. Section II describes the ARS framework while the reputation model is presented in Section III. Some results for a simulated mobility scenario are shown in Section IV, while Section V presents related work. Finally, in Section VI some conclusions are drawn.

## II. The Agent-based Reputation System (ARS)

In this section, the proposed framework ARS is described in detail. We assume that each ARS agent is provided of suitable computational and storing capabilities and it is equipped with a pair of cryptographic keys belonging to a Public Key Infrastructure (PKI) [20] (used for authentication aims and for assuring the communication privacy when it is necessary).

Within ARS, information can be provided for free or for pay. For convenience, we denote as *producer* ($p$) those agents acting as information sources, while the agents consuming information will be denoted as *consumer* ($c$). Note that when an ARS agent plays both the roles of consumer and producer (usually identified as a prosumer) then it will have a different reputation score for each one of these two roles. Moreover, in ARS information could be provided for free or for pay (based on a real or a virtual currency) or, in other words, agents can be benevolent or acting for an economic interest.

More in detail, the four adopted typologies of agents are:

- A *Manager Agent* (MA) is a trusted agent and safe element collaborating with the other agents. All the MAs are mutually connected and provide the other agent of an identifier, unique in the system, and makes available same basic services to the agents, for instance a yellow pages service.
- A *Bridge Agent* (BA) is a trusted agent associated with an infrastructural component belonging to the ARS transport network. All the BAs are mutually connected and spread information among the vehicle agents when, for some reason, vehicle-to-vehicle communication are impossible to carry out in real time, e.g. for a temporary failure (see Section III).
- A Vehicle Agent (VA) is the first of the two agents associated with each vehicle. A VA is free of entering and/or leaving (i.e., it becomes active or not on) the transport network at any time and supports the vehicle owner in his/her activities.
- A Stub Agent (SA) is the other agent associated with a vehicle and managing, in an exclusive way, the reputation information and its safe transmission. It is a trusted tamper-proof component of the MA that is hosted on a vehicle and it is not manipulable, in any way, by the vehicle owner. It becomes active together with the VA.

In the following, $v_x^p$ is the VA acting as a producer of information, associated with the agent of the generic vehicle $x$, and similarly $v_y^c$ is the VA acting as an information consumer, associated with the agent of the generic vehicle $y$. The tasks carried out by VA are identified as (*i*) *Affiliation* and (*ii*) *Supporting*. More in detail:

- **Affiliation**. In ARS each VA has to be registered, also by using reliable and verified third parties. In turn, a MA will provide this agent with an identifier (unique in ARS), a SA and two initial reputation scores (i.e., $\mathcal{R}p$ and $\mathcal{R}c$ stored by the SA), the first one is referred to the trustworthiness of the VA as producer and the other one as consumer. As stated before, two different reputation scores are considered because the producer and the consumer reputations generally do not overlap.
- **Supporting**. Each VA manages all the tasks involving *i*) its identity and *ii*) the interactions with the other agents. These latter tasks, in turn, can be grouped into two sets of activities carried out by a VA, respectively named *Communication Management* and *Resource Provisioning*. More in detail, the *Communication Management* set includes:
  - *Activation.* Whenever a VA enters or leaves (i.e., it becomes active or inactive on) ARS, then it informs one of the MAs.
  - *Presentation.* When a VA is active in ARS, it periodically informs of its presence, in a polling way, all the agents in its neighboring. Furthermore, each VA maintains an updated list of the agents active in its neighboring.
  - *Information request.* When $v_y^c$ searches for information, its SA agent sends a signed $Request$ message to the agents in its neighboring. More in detail, the $Request$ message is formed by the tuple $\langle Id_y, \mathcal{R}c_y, CH_y, D_y^i \rangle$, where: $Id_y$ is the identifier of $v_y^c$; $\mathcal{R}c$ is the reputation score of $v_y^c$; $CH_y$ is the *Consumer Hazard* [21]–[23] autonomously set by the owner of $y$, which represents the minimum reputation score required to a producer for starting with an interaction; $D_y^i$ is the descriptor of the $i$-th searched information resource.
  - *Information offering.* This stage is carried out only when the information has a real (or virtual) price. In this case, if $v_x^p$ satisfies the $v_y^c$ requirements, included $CH_y$, while the reputation of $v_y^c$ is greater than a suitable threshold value named *Producer Hazard* ($PH_x$) –which represents the minimum reputation score required by $x$ to a consumer for starting with an interaction– then $v_x^p$ prepares a message, named $Offering$, formed by the tuple $\langle Id_x, \mathcal{R}p_x, pr_x, D_y^i \rangle$, where: $Id_x$ is the identifier of $v_x^p$; $\mathcal{R}p$ is the reputation score of $v_x^p$; $pr_x$ is the price of the information offered by $v_x^p$; $D_y^i$ is the descriptor of the required information resources. This message is signed by the SA associated with $v_x^p$ and sent to the SA of $v_y^c$.

*Resource Provisioning.* Once the required information is available, if it is provided:

- *For free*. $v_x^p$ sends the resource to $v_y^c$.
- *For pay*. $v_y^c$ signs with its private key one of the received $Offering$ messages and returns it (with the payment of the resource) to the chosen producer that, in turn, makes accessible the information.

Once this phase ends, the involved SAs compute and exchange with their counterparts the respective feedbacks and then update the reputation scores of their associated VAs, as explained in the next Section.

## III. The Reputation Model

In [24] reputation is defined as "*... an expectation about the user's behavior based on information about the observations of her/his past behavior.*"; In line with this definition, in the proposed model a reputation score considers the whole past history of each producer/consumer by taking into account the feedbacks assigned to it by its counterparts [25]. More in detail, when an *Information Provisioning* task ends, the involved SAs mutually exchange the *feedbacks* referred to the behaviors of the counterparts to update the respective VA reputation scores. Note that the SAs carry out the same activities independently on the played role. For such a reason, in the following two generic SAs, named $s_i$ and $s_j$, which manage feedbacks and reputation scores, will be considered.

Now, let $f_{j,i}^I \in [0,1] \subset \mathbb{R}$ be the feedback about $VA_i$ for the information $I$ (where $0/1$ means the minimum/maximum appreciation for $VA_i$). After the feedback $f_{j,i}^I$ has been sent by $s_j$ to $s_i$, this latter calculates the value of the parameter $K_{j,i}^I$ as:

$$K_{j,i}^I = \frac{1}{2} \cdot \left(\widehat{C}^I + q_{j,i}\right) \cdot {f_{j,i}}^I \cdot h_j$$

where $K_{j,i}^I$ takes into account some parameters depending on: *i*) the real (or virtual) cost of the information $I$; *ii*) the number of the interactions occurred in the past between $VA_i$ and $VA_j$ (i.e., $q\ ^I$); *iii*) the feedback given by $s_j$ about $VA_i$ for $I$ (i.e., ${f_{j,i}}^I$); *iv*) the capability of $VA_j$ to provide correct feedbacks (i.e., $h_j$).

The agent $s_i$ will update the current reputation score of $VA_i$ (i.e., ${R_i}^{old}$), and its credential, only if the condition $K_{j,i}^I > 0 \vee R_{old}^i \geq 0.5$ is satisfied (it is a countermeasure against malicious behaviors ruled by the parameters $q$ and $c$, see below) as:

$$ {R_i}^{new} = w \cdot {R_i}^{old} + (1-w) \cdot K_{j,i}^I \qquad (1)$$

where the weight $w \in [0,1] \subset \mathbb{R}$ of Eq. (1) assignes the relevance of the old reputation score with respect to the new contribution represented by the parameter $K$. The higher is the value of $w$, the lower will be the sensitivity of the reputation to a high value of $K$. Otherwise, the updating is not executed, i.e. ${R_i}^{new} = {R_i}^{old}$.

Note that to contrast whitewashing strategies [26] the reputation is initially fixed to 0.5 to avoid of penalizing the newcomers [27].

**The parameter** $\widehat{C}$ - The parameter $\widehat{C}$ takes into account the cost $C^I$ of the information $I$ (Eq. 2), where $C_{Max}$ represents the maximum cost threshold; in presence of cost higher than $C_{Max}$ then $\widehat{C}^I$ is set to 1. Therefore, the effect of the feedback in updating the reputation depends tightly on the cost payed for $I$. This limits the alternate behavior devoted to gain reputation in presence of low costs for spending it by cheating in presence of high costs. When $I$ is for free the parameter $\widehat{C}$ is set to 1.

$$\widehat{C}^I = \begin{cases} 1 & \textit{for free} \\ Min\left(1, \dfrac{C^I}{C_{Max}}\right) & \textit{for pay} \end{cases} \qquad (2)$$

**The parameter** $q$. This parameter is effective against collusive behaviors aimed to increase maliciously the reputation scores by exploiting positive feedbacks, mutually exchanged with high frequency among one or more participants. This activity is hindered by means of the action of the parameter $q$ which is computed as:.

$$q_{j,i} = \begin{cases} 1 & f_{j,i}^I < 0.5 \vee T_{j,i} = 1 \\ \dfrac{1}{1+e^{(1-T_{j,i})}} & f_{j,i}^I \geq 0.5 \wedge T_{j,i} > 1 \end{cases} \qquad (3)$$

where $q$ is set to 1 when $f_{j,i} < 0.5$ (i.e., a negative appreciation). On the contrary, in the case of a positive or neutral appreciation, the value of $q$ is given by the expression $1/(e^{(1-T_{j,i})})$, where the parameter $T_{j,i}$ depends on the time occurring between two consecutive interactions between $s_j$ and $s_i$ evaluated positively. In particular, let $t_l$ and $t_p$ be the timestamps of the last and the second to last positive feedbacks and let $\Delta T$ be a suitable time threshold. With the first positive feedback $T_{i,j}$ is set to 1 (i.e., $T_{i,j} = 1$) then, for each further positive feedback, *i*) if $(t_l - t_p) < \Delta t$ then $T_{i,j}$ is increased by 1 (i.e., $T_{i,j} = T_{i,j} + 1$), otherwise *ii*) if $(t_l - t_p) \geq \Delta t$ then $T_{i,j}$ is set to $Max\left(1, T_{j,i} - \left\lfloor \frac{t_l - t_p}{\Delta t} \right\rfloor\right)$.

**The parameter** $h$. It takes into account the honesty in providing correct feedbacks. The value of this parameter is computed by the SAs with an uniform metric. More specifically, $h \in [0,1] \in \mathbb{R}$ where 1 identifies a completely "honest" member and vice versa for 0. The computation of $h$ is obtained as:

$$ {h_j}^{new} = p \cdot {h_j}^{old} + (1-p) \cdot \left(1 - |{f_{j,i}}^I - R_i|\right) \qquad (4)$$

where the parameter $p$ weights the relevance of $h^{old}$ with respect to the new contribution computed by considering the difference between the feedback provided and the reputation of the target agent. In this way, when this difference is zero the value of the parameter $h$ is maximum.

**Self storage reputation.** Differently from other proposals [28], in ARS each SA (which is a tamper-proof component) stores the reputation informations of its hosts in a trusted way. This solution avoids the typical problems in knowing

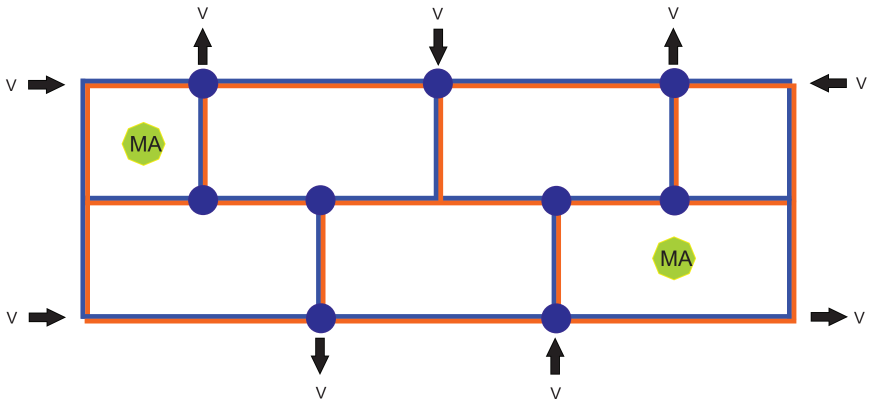

Fig. 1. The transportation network

the reputation scores due to their poor spreading into the community (in the distributed approaches) or for temporary failure of the server (in the centralized approaches).

**Communication failures.** In presence of a communication failure the feedbacks cannot be exchanged and the reputation scores cannot be updated. For instance, think to a malicious behavior addressed to avoid a negative evaluation or a communication failure. As a consequence, the SA could penalize the reputation score of its host by ${R_i}^{new} = z \cdot {R_i}^{old}$, with $z \in [0,1] \in \mathbb{R}$. More specifically, if a malicious behavior is recognized by a SA then it will penalize its host by randomly setting $z$ in $[0, 0.5[$; otherwise, when it is impossible to confirm or to exclude a voluntary communication failure, the involved SAs will provide to penalize their hosts by randomly setting $z$ in $]0.5, 1]$ with a probability $p_c = 0.5$.

However, in this latter case, the penalizing process is a rare event given the presence of the BAs placed on the transport network. The BAs are interconnected among them and can overcame a temporary communication failure by acting as a common repository among the agents.

## IV. The Case Study

We tested ARS and its reputation model by simulating a mobility scenario on a small transportation network [29]–[32], see Figure 1. In this case study two MAs managing the ARS are considered and two different contexts, respectively named $A$ and $B$, were tested. Both $A$ and $B$ consider 1000 vehicles, 9 BAs associated with the 9 traffic-lights placed on the transportation network [33] and assumed the 10% of the VAs as malicious. For sake of simplicity, the interactions vehicle-to-vehicle are assumed occurring when they are stopped at traffic-lights without this affects the simulations results.

Moreover, we supposed that information on the local state of the transportation network and on the reliability of the information sources cannot be exchanged together. This makes more difficult the agent communications and, for such a reason, we assumed that the SAs require the support of the BAs with a probability $p_f$. In other words, the lost messages can be recovered by means of the BAs associated with the next traffic-lights encountered by the vehicles.

To obtain stable and significant trends for both the scenarios, the simulations run for 80 epochs. Moreover, for each epoch only 25% of the vehicles, randomly chosen, were active on the network. Scenario $A$ is characterized by low performances because of communication failures (with probability $p_f$) due to malicious agents (penalized with probability $p_c$) which also release low feedbacks to reliable counterparts and vice versa. In scenario $B$ the malicious behaviors are addressed to build a positive reputation with a correct behavior, in presence of low cost information, for spending it by cheating in presence of expensive information. The scenario $B$ assumes that this alternate behavior happens the 25% of the time, this means that each three low cost information (i.e, correct behaviors) there is an expansive one (i.e., cheating behavior).

All the initial reputation values were set to 0.5. This value is the border between reliability and unreliability so that unreliable behaviors are defined by feedbacks lower than 0.5. In Table I the setting of $\Delta t$, $w$, $p$, $p_f$, $p_c$ and of the green/red ($g/r$) traffic-light cycles (obtained by some preliminary tests) is shown, while the vehicle speed was chosen in the range $[25, 50]$ $Km/h$ in a random way.

In the simulation, to verify the effectiveness of the proposed system, the ratio of *malicious* agents and their Average Reputation, respectively referred as $M$ and $\overline{R}$, have been measured. Figure 2 depicts these measures for both scenarios. More in detail, for scenario $A$, when the number of interactions is significant (e.g., 26 epochs) about 90% of the malicious agents have been correctly identified (i.e., $M_A$) and have a value lower than 0.5, see curve $\overline{R}_A$, which starts from the initial values of 0.5 and decreases as the number of epochs increases. Scenario $B$ shows similar results (i.e., $M_B$ and $\overline{R}_B$) to those of scenario $A$ and, therefore, the reputation model shows its

TABLE I
Parameters Setting

| $\Delta t$ | $w$ | $p$ | $p_f$ | $p_c$ | $g/r$ |
|---|---|---|---|---|---|
| 5 | 0.5 | 0.5 | 0.2 | 0.5 | 1<br>$i.e.$, 60/60 $sec.$ |

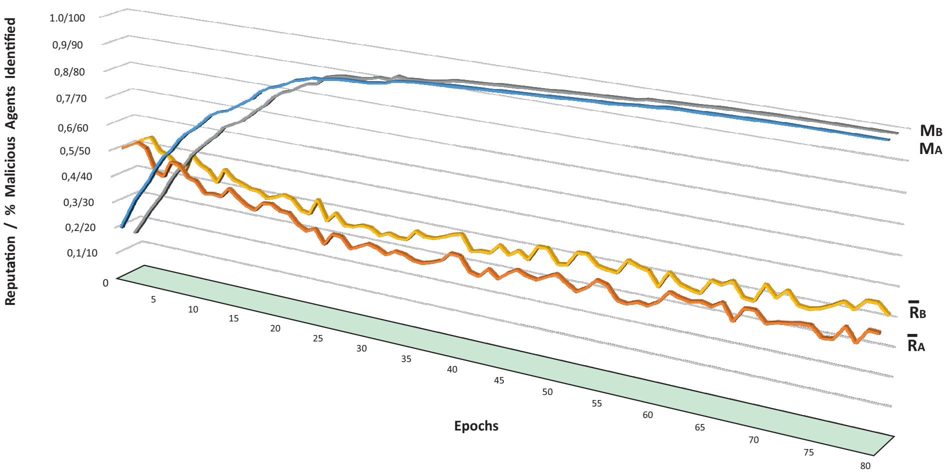

Fig. 2. $M$ and $\overline{R}$ measures for unreliable agents (80 epochs). Scenarios A and B.

resilience also with respect to a dynamic agent behavior.

Then the results of this preliminary experimental session confirm that the proposed system and reputation model work correctly and the unreliable agents are identified quickly (without "false positive"), while ARS is capable to suitably support all the activities of the different agents.

## V. Related Work

A significant amount of works exploit reputation and trust systems. In this paper some of them, that at best of our knowledge come close to the matter presented here, will be discussed in this section.

In [34] users search/offer information, within the communication range of their mobile devices, driven by the trustworthiness of their potential counterparts. To this purpose, two different reputation systems are adopted. The first one exploits a common centralized mechanism, while the other one is a distributed system managed by trusted local components, named observers, which spread reputation information among mobile users by using cryptographic techniques in order to preserve privacy.

Reputation systems are popular within P2P contexts and are widely adopted as, for instance, in PeerTrust [35] where more strategies against malicious users and their attacks are implemented by storing, locally at each peer, the reputation information that are suitably spread when the peers interact. Another example is described in [36], where mobile and heterogeneous peers have to interact on limited (for range) and unreliable communication channels. The best available connectivity is chosen in real time on the basis of both a reputation system on seven metrics and a polling protocol. Similarly, in RLoad [37] the mobile network having the best traffic load balancing is chosen by using reputation measures.

Often the Ad-Hoc networks have to deal with misbehavior and selfishness nodes and, to this aim, in [38] a reputation-based system is proposed to enforce cooperation among nodes. In this system, nodes maintain the memory of their past partners and more information sources are exploited to compute the reputation score of their potential partners. However this system is not able to contrast some attack typologies and does not consider negative feedbacks. To recognize misbehaving peers, in [39] a dynamic trust management protocol for smart nodes which combines accuracy and resilience properties is proposed. The results of some simulations have shown that it adjusts its trust parameters in responding to dynamical environmental changes. The authors of [40], in a mobile IoT scenario, designed a model providing a trusted authentication of the service providers by using an agent approach. This trust model assigns users' trustiness to one of three trust classes (i.e., high, medium and low) to suggest the more appropriate authentication method.

To summarize, the considered works adopt trust and reputation systems (also locally managed) in order to evaluate the potential counterparts and, in some cases, also exploit cryptographic techniques to assure integrity of both trust/reputations and identities informations. Other aspects considered in this papers are the initial trust/reputation scores assigned to newcomers, the reputation dissemination and service availability. However, all the cited system have some (but not all) the features of ARS which, differently from them can work with good performances indifferently in benevolent or competitive vehicle-to-vehicle communication scenarios (i.e., by exchanging information for free or paying), notwithstanding the limited complexity of its reputation model.

## VI. Conclusions and Future Work

In this paper we presented a reputation agent model to assure the reliability of the information sources in vehicle-to-vehicle interactions. To this aim, an agent-based reputation system, named ARS, and a reputation model have been suitably designed to make ineffective or limiting the effects of malicious and collusive activities Preliminary experiments carried out on a simulated scenario tested the effectiveness of this proposal. Our ongoing researches are addressed to realize a wider simulation for better investigating on the advantages of ARS also with respect to other known approaches [41], [42] and by testing different settings of the parameters in the reputation model.

## Acknowledgment

This study has been supported by **NeCS** Laboratory (DICEAM, University Mediterranea of Reggio Calabria).

## References

[1] F. Behmann and K. Wu, *Collaborative internet of things (C-IoT): For future smart connected life and business*. John Wiley & Sons, 2015.

[2] J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami, "An information framework for creating a smart city through internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 112–121, 2014.

[3] R. Giunta, F. Messina, G. Pappalardo, and E. Tramontana, "Providing qos strategies and cloud-integration to web servers by means of aspects," *Concurrency and Computation: Practice and Experience*, vol. 27, no. 6, pp. 1498–1512, 2015.

[4] P. De Meo, F. Messina, D. Rosaci, and G. M. L. Sarné, "Improving grid nodes coalitions by using reputation," in *Intelligent Distributed Computing VIII*. Springer, Cham, 2015, pp. 137–146.

[5] M. Abomhara and G. M. Køien, "Security and privacy in the internet of things: Current status and open issues," in *Privacy and Security in Mobile Systems (PRISMS), 2014 Int. Conf. on*. IEEE, 2014, pp. 1–8.

[6] L. Mui, M. Mohtashemi, and A. Halberstadt, "Notions of reputation in multi-agents systems: a review," in *Proc. 1st int. conf. on Autonomous agents and multiagent systems*. ACM, 2002, pp. 280–287.

[7] B. Misztal, *Trust in modern societies: The search for the bases of social order*. John Wiley & Sons, 2013.

[8] 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 *Networking, Sensing and Control (ICNSC), 2017 IEEE 14th International Conference on*. IEEE, 2017, pp. 513–518.

[9] M. N. Postorino and G. M. L. Sarné, "Mobility forecast in an urban area through the use of neural networks," in *Applications of advanced technologies in transportation engineering*. ASCE, 1995, pp. 213–217.

[10] E. Picasso, M. N. Postorino, and G. M. L. Sarné, "A study to promote car-sharing by adopting a reputation system in a multi-agent context," in *Proceedings of the 18th Workshop dagli Oggetti agli Agenti, WOA 2018*, ser. CEUR Workshop Proceedings, vol. 1867. CEUR-WS.org, 2017.

[11] M. D. Dikaiakos, A. Florides, T. Nadeem, and L. Iftode, "Location-aware services over vehicular ad-hoc networks using car-to-car communication," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, 2007.

[12] L. Mantecchini and F. Paganelli, "Airport ground access and urban congestion: A paradox of bi-modal networks," *Contemporary Engineering Science*, vol. 9, pp. 1491–1501, 2016.

[13] U. Tang and Z. Wang, "Influences of urban forms on traffic-induced noise and air pollution: Results from a modelling system," *Environmental Modelling & Software*, vol. 22, no. 12, pp. 1750–1764, 2007.

[14] S. Biswas, R. Tatchikou, and F. Dion, "Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety," *IEEE communications magazine*, vol. 44, no. 1, pp. 74–82, 2006.

[15] M. N. Postorino and G. M. L. Sarné, "Agents meet traffic simulation, control and management: A review of selected recent contributions," in *Proceedings of the 17th Workshop dagli Oggetti agli Agenti, WOA 2016*, ser. CEUR Workshop Proceedings, vol. 1664. CEUR-WS.org, 2016.

[16] A. Jøsang, E. Gray, and M. Kinateder, "Simplification and analysis of transitive trust networks," *Web Intelligence and Agent Systems: An International Journal*, vol. 4, no. 2, pp. 139–161, 2006.

[17] J. Kaur, S. Saxena, and M. A. Sayeed, "Securing mobile agent's information in ad-hoc network," in *Confluence The Next Generation Information Tech., 2014 5th Int. Conf.* IEEE, 2014, pp. 442–446.

[18] E. Cascetta and M. N. Postorino, "Fixed point approaches to the estimation of o/d matrices using traffic counts on congested networks," *Transportation science*, vol. 35, no. 2, pp. 134–147, 2001.

[19] M. Postorino, G. Musolino, and P. Velonà, "Evaluation of o/d trip matrices by traffic counts in transit systems," in *Schedule-Based Dynamic Transit Modeling: theory and applications*. Springer, 2004, pp. 197–216.

[20] C. Adams and S. Lloyd, *Understanding PKI: concepts, standards, and deployment considerations*. Addison-Wesley Professional, 2003.

[21] R. Falcone and C. Castelfranchi, "Social trust: A cognitive approach," in *Trust and deception in virtual societies*. Springer, 2001, pp. 55–90.

[22] F. Perich, J. Undercoffer, L. Kagal, A. Joshi, T. Finin, and Y. Yesha, "In reputation we believe: query processing in mobile ad-hoc networks," in *Mobile and Ubiquitous Systems: Networking and Services, 2004. The 1st Annual Int. Conf. on*. IEEE, 2004, pp. 326–334.

[23] Y.-H. Tan and W. Thoen, "An outline of a trust model for electronic commerce," *Applied Artificial Intell.*, vol. 14, no. 8, pp. 849–862, 2000.

[24] A. Abdul-Rahman and S. Hailes, "Supporting trust in virtual communities," in *System Sciences, 2000. Proc. of the 33rd Annual Hawaii Int. Conf. on*. IEEE, 2000, pp. 9–pp.

[25] P. De Meo, F. Messina, D. Rosaci, and G. M. L. Sarné, "Combining trust and skills evaluation to form e-learning classes in online social networks," *Information Sciences*, vol. 405, pp. 107–122, 2017.

[26] G. Zacharia and P. Maes, "Trust management through reputation mechanisms," *Applied Artificial Intelligence*, vol. 14, no. 9, pp. 881–907, 2000.

[27] S. D. Ramchurn, D. Huynh, and N. Jennings, "Trust in multi-agent systems," *Knowledge Engineering Review*, vol. 19, no. 1, pp. 1–25, 2004.

[28] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision support systems*, vol. 43, no. 2, pp. 618–644, 2007.

[29] M. N. Postorino, "A comparative analysis of different specifications of modal choice models in an urban area," *European journal of operational research*, vol. 71, no. 2, pp. 288–302, 1993.

[30] M. N. Postorino and V. Fedele, "The analytic hierarchy process to evaluate the quality of service in transit systems," *WIT Transactions on The Built Environment*, vol. 89, 2006.

[31] M. N. Postorino and M. Versaci, "A neuro-fuzzy approach to simulate the user mode choice behaviour in a travel decision framework," *International Journal of Modelling and Simulation*, vol. 28, no. 1, pp. 64–71, 2008.

[32] M. N. Postorino, V. Barrile, and F. Cotroneo, "Surface movement ground control by means of a gps–gis system," *Journal of Air Transport Management*, vol. 12, no. 6, pp. 375–381, 2006.

[33] M. N. Postorino and M. Versaci, "Upgrading urban traffic flow by a demand-responsive fuzzy-based traffic lights model," *International Journal of Modelling and Simulation*, vol. 34, no. 2, pp. 102–109, 2014.

[34] M. Voss, A. Heinemann, and M. Muhlhauser, "A privacy preserving reputation system for mobile information dissemination networks," in *1st Int. Conf. on Security and Privacy for Emerging Areas in Communications Networks*. IEEE, 2005, pp. 171–181.

[35] 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, no. 7, pp. 843–857, 2004.

[36] X. Wu, "A distributed trust evaluation model for mobile p2p systems," *Journal of Networks*, vol. 7, no. 1, pp. 157–164, 2012.

[37] T. Bi, R. Trestian, and G.-M. Muntean, "Rload: Reputation-based load-balancing network selection strategy for heterogeneous wireless environments," in *2013 21st IEEE Int. Conf. on Network Protocols (ICNP)*. IEEE, 2013, pp. 1–3.

[38] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Advanced communications and multimedia security*. Springer, 2002, pp. 107–121.

[39] 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*, ser. Self-IoT '12. New York, NY, USA: ACM, 2012, pp. 1–6. [Online]. Available: http://doi.acm.org/10.1145/2378023.2378025

[40] Y. Liu, Z. Chen, F. Xia, X. Lv, and F. Bu, "A trust model based on service classification in mobile services," in *Proc. of the 2010 IEEE/ACM Int. Conf. on Green Computing and Comm. & Int. Conf. on Cyber, Physical and Social Computing*. IEEE Computer Society, 2010, pp. 572–577.

[41] M. N. Postorino and M. Versaci, "Modelling user mode choices by an ellipsoidal fuzzy approach," *International Journal of Modelling and Simulation*, vol. 33, no. 4, pp. 235–243, 2013.

[42] M. N. Postorino and G. M. L. Sarné, "An agent-based sensor grid to monitor urban traffic," in *Proceedings of the 15th Workshop dagli Oggetti agli Agenti, WOA 2014*, ser. CEUR Workshop Proceedings, vol. 1260. CEUR-WS.org, 2014.