Hindawi
Wireless Communications and Mobile Computing
Volume 2017, Article ID 7089259, 11 pages
https://doi.org/10.1155/2017/7089259

Research Article

Trust on the Ratee: A Trust Management System for Social Internet of Vehicles

Fangyu Gai,[1] Jiexin Zhang,[1] Peidong Zhu,[2] and Xinwen Jiang[3]

[1]*School of Computer, National University of Defense Technology, Changsha, China*
[2]*Department of Electronic Information and Electrical Engineering, Changsha University, Changsha, China*
[3]*The MOE Laboratory of Intelligent Computing & Information Processing, Xiangtan University, Xiangtan, China*

Correspondence should be addressed to Peidong Zhu; pdzhu@nudt.edu.cn

Received 2 August 2017; Accepted 19 November 2017; Published 10 December 2017

Academic Editor: Zhipeng Cai

The integration of social networking concepts with Internet of Vehicles (IoV) has led to the novel paradigm "Social Internet of Vehicles (SIoV)," which enables vehicles to establish social relationships autonomously to improve traffic conditions and service discovery. There is a growing requirement for effective trust management in the SIoV, considering the critical consequences of acting on misleading information spread by malicious nodes. However, most existing trust models are rater-based, where the reputation information of each node is stored in other nodes it has interacted with. This is not suitable for vehicular environment due to the ephemeral nature of the network. To fill this gap, we propose a Ratee-based Trust Management (RTM) system, where each node stores its own reputation information rated by others during past transactions, and a credible CA server is introduced to ensure the integrality and the undeniability of the trust information. RTM is built based on the concept of SIoV, so that the relationships established between nodes can be used to increase the accuracy of the trustworthiness. Experimental results demonstrate that our scheme achieves faster information propagation and higher transaction success rate than the rater-based method, and the time cost when calculating trustworthiness can meet the demand of vehicular networks.

1. Introduction

This is an extension of the paper titled "Ratee-Based Trust Management System for Internet of Vehicles" [1]. Internet of Vehicles (IoV) is a new paradigm brought by the integration of Vehicular Ad hoc NETworks (VANETs) and Internet of Things (IoT) in the last few years [2]. VANETs enabling vehicles to connect with each other result in networks with wide range [3]. However, VANETs cannot provide global and sustainable services for users. Over the last few decades, there has not been any successful implementation of VANETs. In contrast to VANETs, IoV has two main technology directions [4]: (1) vehicles' networking, which consists of VANETs, Vehicle Telematics, and Mobile Internet; (2) Vehicles' intelligence, which is the integration of drivers and intelligent vehicles by applying technologies such as deep learning, cognitive computing, and artificial intelligence. IoV consists of two types of communications: Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Infrastructure (V2I) communication, which enable tremendous applications ranging from safety to entertainment and commercial services [5]. With the help of IoV, vehicles can not only be aware of the conditions on the road but also request services from other vehicles, such as live video from other vehicles' recorders. In addition, vehicles in the network can communicate with each other by switching real-time information about road and traffic conditions, so that they can avoid car accidents and effectively route traffic through dense urban areas. In the near future, there will be fewer direct interactions between vehicles and humans, and vehicles can build their own relationship with each other to get better service and enhance the safety of the whole network.

As it is in Mobile Ad hoc NETworks (MANETs), trust problem is a major concern in VANETs and IoV. The trustworthiness in VANETs is defined as the assessment of whether or not and to what extent the node in VANETs can be

trusted. The motivation of constructing a trust management system for IoV is evident: (1) Malicious nodes may spread misleading information to break the core functionality of the IoV system; (2) there are also many socially uncooperative nodes refusing to provide services to others for selfishness reasons. Considering the dire consequences of false information being sent out by malicious nodes in this scenario, building an effective trust management system for IoV is of paramount importance.

In the last few years, there is a trend to integrate social networking concepts with Internet of Things (IoT) solutions, and a new paradigm named "Social Internet of Things (SIoT)" is gaining momentum. In [6], the researchers believe that applying social networking principles to IoT can improve network navigability and boost the process of discovery of objects and services. In [7], two trust models (the subjective model and the objective model) are defined for trustworthiness management based on solutions proposed for P2P and social networks. In [2], the authors analyzed the combination of VANETs with SIoT and proposed a Social Internet of Vehicles (SIoV) middleware which extends the functionalities of the Intelligent Transportation Systems Station Architecture (ITS SA). Alam et al. [8] presented a vehicular social network platform following cyber-physical architecture. In their cyber-physical SIoV system, social relationships among physical components are applied to encourage different types of communications, and the information is stored as a social graph.

It is challenging to evaluate trust in vehicular networks because it needs past transaction information to compute trust values of the target node. Due to the ephemeral nature of vehicular networks, it is not guaranteed for one node to interact with the same vehicle more than once. Furthermore, gathering trust information from past transactions is computationally expensive, which introduces another big challenge. To tackle these problems, we propose a *Ratee-based* Trust Management system. Current trust models are mostly *rater-based*, where each node stores trust information about the nodes it has interacted with [7]. In these models, once a node has contacted with an unknown node, it has to ask other nodes for trust opinions. This procedure can last for a long time, which is not efficient, and the situation can get even worse if no nodes nearby have ever interacted with that unknown node. Therefore, rater-based methods are not suitable for the ephemeral nature of vehicular networks.

However, in our proposed *ratee-based* model, each node stores its own reputation information recorded during the past transactions. When interaction happens, the requester can read trust information from the provider and compute trust value afterward. Some relationships such as *Parental Object Relationship* (POR), *Social Object Relationship* (SOR), and *Co-Work Object Relationship* (CWOR) defined by SIoV [2] will be used in our system for trust evaluation.

The rest of the paper is organized as follows. Section 2 introduces the related work about Social Internet of Vehicles and reputation mechanisms in VANETs. Section 4 describes the details of our system. In Section 5, we demonstrate the evaluation results of our system experimentally. We conclude in Section 6 and point out the directions for future work.

2. Related Work

Our model is based on SIoV [2]. In this section, we will describe state of the art in Social Internet of Vehicles and reputation mechanisms in VANETs.

2.1. The Social Internet of Vehicles. With the development of IoT technology, more and more smart objects are emerging in our daily life. In the last few years, the idea of integrating social networking theories into IoT to allow objects to establish social relationships autonomously has drawn researchers' attention. The novel concept of "Social Internet of Things" is firstly defined in [9], which is based on the notion of social relationships among objects.

The establishment of relationships among objects in vehicular networks is simpler because of fewer types of objects. In [2], the concept of SIoT is extended to the IoV, which results in a novel paradigm called Social Internet of Vehicles (SIoV). This concept introduces a social network of intelligent vehicles, where vehicles can establish social relationships and exchange information to improve the driving experience and provide various services to the users.

In SIoV, the mobile nodes are vehicles equipped with an On-Board Unit (OBU), and the static nodes are roadside units (RSUs). The communication between vehicles is called Vehicle-to-Vehicle (V2V) communication. The communication between vehicles and RSUs is called Vehicle-to-Infrastructure (V2I) communication [10]. Besides, the vehicles and the RSUs are assumed to be able to connect to the Internet by using mobile cellular systems. In [8], the architecture of SIoV is described as three layers (Figure 1): physical layer, cyber layer, and social layer. Physical layer consists of physical entities (vehicles with OBUs and RSUs). Every physical entity has its corresponding twin cyber entity which is described in the cyber layer. The social layer can be considered as an overlayer of VANETs, and, based on [6], three typical types of social relationships in SIoV are defined as follows.

(1) Parental Object Relationship (POR): POR describes relationships that vehicles belong to the same manufacturer. These relationships can help users find available information about the status of a vehicle or solve problems which had happened to others before.

(2) Social Object Relationship (SOR): SOR describes relationships that vehicles come into contact with each other through V2V communication. SORs are the most common relationships in SIoV. For example, after the first interaction, two nodes will establish an SOR relationship, and the trust will accumulate as the number of interactions between the two nodes grows.

(3) Co-Work Object Relationship (CWOR): CWOR describes relationships between vehicles and RSUs. RSUs can contact with vehicles when they are within the scope. So CWORs can help provide traffic information or guide the drivers to their destinations in less congested routes.

The benefits of establishing these relationships are important in SIoV, which is the core idea in our trust model.

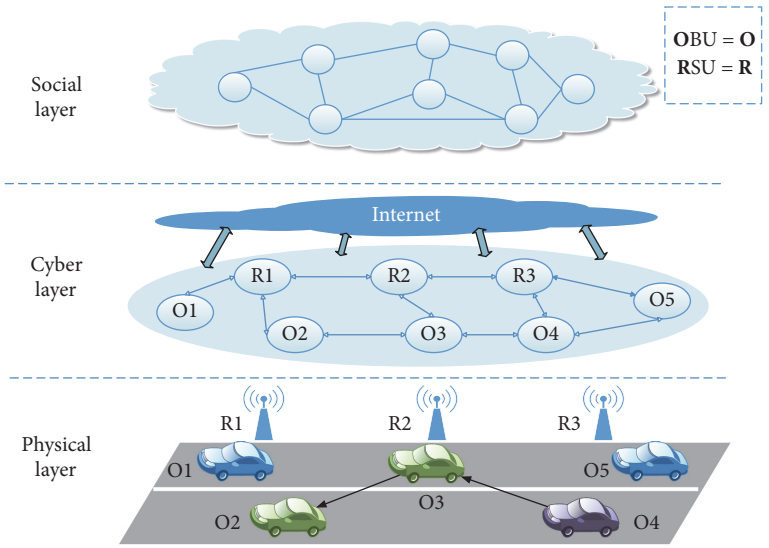

Figure 1: Abstract architecture of Social Internet of Vehicles (SIoV).

Nitti et al. [7] propose two trustworthiness management models (the subjective model and the objective model), which is the first trust model for SIoT. The objective model is derived from P2P communication networks. The trust value of each node is stored and retrieved in a distributed hash table to realize global sharing. The subjective model is derived from social networks, with each node computing the trust values of its friends based on its own experience and the opinion of its friends. Both of the two models are not beneficial to be applied in SIoV directly, because of the ephemeral nature of vehicular networks. To apply trust management in SIoV, we propose a novel ratee-based method which will be detailed in Section 4.

2.2. Trust Management in VANETs. The study of trust management in MANETs has reached maturity in the last decade [11–13], and the main purpose of applying trust management in MANETs is to encourage node cooperation and punish selfishness. The estimation of trust values usually relies on two sorts of observations of node behaviors which are first-hand observation and second-hand observation [14]. First-hand observation is the observation about the node's direct experience. It can be collected either passively or actively. While second-hand observation is the observation about other nodes' indirect opinions. It is generally obtained by exchanging first-hand observations with other nodes in the network. First-hand and second-hand observation will be assigned different weights according to different scenarios when evaluating trust values.

However, as one of the specific applications in MANETs, VANETs bring new challenges to trust evaluation. Compared to MANETs, VANETs are ephemeral, short-duration wireless networks. The size of VANETs is larger, which may contain millions of vehicles. So the network traffic could be high in the dense area. The topology of VANET is dynamic since nodes contact with each other at high speed. In [15], the authors propose a list of desired properties that effective trust management should incorporate for VANETs, some of which are important but not carefully concerned:

(1) Decentralized trust establishment: trust establishment should be fully decentralized due to the highly dynamic and distributed environment of VANETs.

(2) Coping with sparsity: in VANETs, there is no guarantee that one node will possibly interact with other nodes more than once. Even though the direct interaction between two nodes might happen just once, it is important that the trust models should still take any data available into consideration as much as possible.

(3) Being scalable: scalability is an important property in trust management in VANET environments, because in urban areas the network can be expanded very large, which results in high network traffic. So nodes have to interact with only a few number of other nodes. An efficient trust management system should ensure that number is set to a small value to account for scalability.

(4) Being sensitive to privacy concerns: privacy is a significant concern in VANETs. It is a potential threat that private information is exposed in the public. Furthermore, people may feel uncomfortable seeing others rate them with low trust values. Hence, some pseudonym mechanism is necessary for VANETs.

(5) Robustness: detecting malicious nodes is one of the main tasks of trust management. However, trust management itself may be targeted by some common attacks such as Sybil attack, newcomer attack, and bad-mouthing attack. Therefore, there should be defense strategy to maintain the robustness of the system.

Only a few trust models have been proposed for trust information sharing in vehicular networks. The state-of-the-art researches on trust models in vehicular networks have

mainly focused on three categories: entity-oriented, data-oriented, and combined trust. Entity-oriented trust models focus on the modeling of the trustworthiness of nodes, and the messages must be authenticated to prevent external attackers. Data-oriented trust models aim to assess the credibility of the reported data. Combined trust models make efficient use of both entity and data trust for authentication of nodes and evaluation of trust [16].

Huang et al. [17] presented a novel trust architecture named Situation-Aware Trust (SAT) to address the trust management issues. SAT focuses on some specific application situations: an event that affects a particular region with immediate processing needs, or a service that has a clear organizational boundary for its users. They also considered the social network as an overlay layer on top of the vehicular communication networks to help reduce the latency of establishing trust and keys. But SAT lacks incentive mechanisms to make selfish nodes cooperate.

In [18], an attack-resistant trust management scheme (named ART) was proposed for VANETs. The authors claimed that their ART can detect and resist malicious attacks such as simple attack, bad-mouth attack, and zigzag attack. They also evaluated the trustworthiness of both data and mobile nodes in VANETs. In the ART scheme, the traffic data from VANETs is collected and used to evaluate the trustworthiness of data and nodes. In addition, the trustworthiness of nodes consists of function trust and recommendation trust, which indicate how likely a node can fulfill its functionality and how trustworthy the recommendations from a node for others will be, respectively. The disadvantage of ART is that data collection and analysis process are time-consuming, and the centralized evaluation is not suitable for the distributed architecture of vehicular networks.

Minhas et al. [19] introduced a multifaceted framework to facilitate the effective interaction in VANETs. Their trust models considered various dimensions and combined these elements effectively to assist agents in making transportation decisions. To increase the accuracy of the trust model, the authors also introduced two elements to the proposed model: distinguishing direct and indirect reports and employing a penalty for malicious reports. A possible drawback of this model is that, in VANET environment, the time is not enough for two agents to establish a trust relationship between them.

Most of the existing trust management methods for vehicular networks are rater-based methods, where each node stores trust information about the nodes it has interacted with. In vehicular networks, it should not be expected that a node would possibly interact with the same node more than once, so it is difficult for a node to ask for recommendation information. Moreover, some of them introduced social network concept into their models, but the effect was not reflected. In this paper, we aim to propose a ratee-based trust model based on SIoV to cope with these problems.

3. Problem and Threat Model

3.1. Problem Definition. The purpose of this study is to provide a new scheme of trust management for IoV by storing the trust evidence in the ratee locally. In RTM, the rater can get recommendations directly from the ratee rather than a group of recommenders, which is cost-efficient.

We formalize the problem of designing a Ratee-based Trust Management system for IoV as follows. Let there be a set of nodes which is represented as $O = \{o_1, \ldots, o_i, \ldots, o_m\}$ with cardinality m, which includes both OBUs and RSUs, because RSUs can be considered as static nodes with high credibility. The vehicular network is described by an undirected graph $G = \{O, E\}$, where $E \subseteq \{O \times O\}$ is the set of edges, each of which represents a social relationship between the set of nodes. Let $S_i = \{o_j \in O : o_i, o_j \in E\}$ be the set of nodes that has a relationship with o_i and $Q_{ij} = \{o_k \in O : o_k \in S_i \cap S_j\}$ be the set of common friends between o_i and o_j. Let $P^i = \{p_1^i, \ldots, p_j^i, \ldots, p_n^i\} \subseteq O$ represent the set of objects from whom o_i received trust evidence, and the cardinality is n.

In our system, OBUs and RSUs are both connected to the Internet. We assume a secure channel between vehicular nodes and servers, so that the trust evidence and identity information would not be intercepted or tampered with. The duration of peer-to-peer communication is short; it is difficult for attackers to intercept or modify messages. Hence, the MITM (Man-in-the-Middle) attack is out of concern. Our trust management system also requires a registry. Vehicular nodes must go through an enrollment process before joining the network. Each node generates a pair of keys using asymmetric cryptography. The public key is submitted to the registry for authentication, while the private key is stored locally for digital signature.

3.2. Threat Model. Trust management system itself is easily targeted by attackers, even if we have assumed that the communication channel is secure. Here we discuss some classic attacks toward trust management systems and our protection.

(i) Slandering attack or bad-mouthing attack, first described by Hoffman et al. [20], is perhaps the most straightforward attack to reputation systems. Attackers deframe good nodes by giving dishonest rating. In our system, each node only keeps the latest trust evidence given by the same node, which can reduce the impact of slandering attack.

(ii) Sybil attack is an attack that can be harmful to all peer-to-peer networks [21]. By performing Sybil attack, attackers "legally" create more than a single identity and therefore they can switch between different IDs to hide their malicious behaviors. To prevent this attack, our system has strict registration management. According to the unique feature of each vehicle, they can only have one identity to join the network.

(iii) On-off attack is to act erratically. Attackers switch between normal mode and attack mode continuously in order to not be detected. In our system, all the trust evidence is recorded in the ratee and cryptographical mechanisms can keep the integrity and reliability.

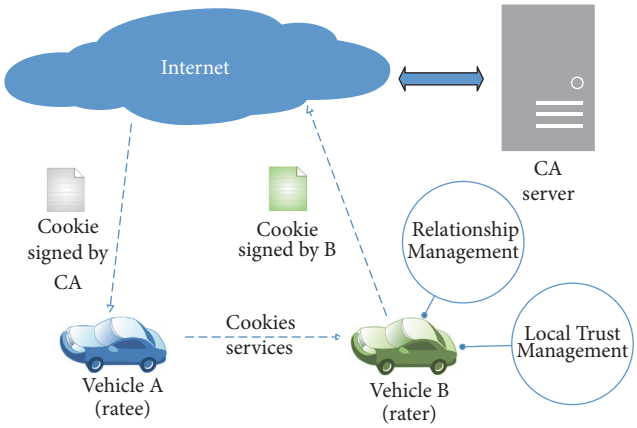

Figure 2: Overall scheme of Ratee-based Trust Management system.

4. System Model

Different from traditional vehicular trust models, RTM is ratee-based, where each node stores a limited amount of information about how much other users trust them, which is to adapt the ephemeral nature of VANETs. RTM is based on SIoV [2], where nodes are capable of establishing social relationships in an autonomous way with respect to their owners. We assume that *Service discovery* in SIoV architecture can give the requester a list of nodes that can provide the demanding service, so we only focus on the trust management part. In this section, we will provide the overall architecture of RTM and describe how the trust management works.

4.1. Architecture. The Ratee-based Trust Management (RMT) system is composed of four components: *CA server*, *Cookies*, *Relationship Management*, and *Local Trust Management*. The schematic diagram of the RTM architecture is depicted in Figure 2. The major procedure of one transaction can be described as follows.

For example, vehicle B is asking for congestion information, and vehicle A is willing to provide the information. To show its trustiness, A sends its *Cookies* which accumulate during past interactions along with the congestion information to B. Note that *Cookie* here is different from the cookie in HTTP that is to identify users. It is a feedback about a transaction generated by the requester and is used to evaluate trust value to the service provider. After receiving the *Cookies* and congestion information, B first checks if the *Cookies* are signed by CA. If so, it computes trust value with these *Cookies* to decide whether to trust A or not. If A can be trusted, then the congestion information will be sent to the application, and after that, a *Cookie* which contains a feedback about this transaction will be generated and sent to the CA Server with a sign from B through the Internet. Then after being verified and signed by CA, the *Cookie* will be sent to A when A connects to the Internet. The details of each component are described as follows:

(1) CA server: the main problem of storing a node's own reputation information locally is that the reputation information can be easily modified or deleted by the owner. So the basic idea of applying CA is to prevent nodes from tampering with their reputation information, that is, *Cookies*. Only a *Cookie* with a sign from CA is valid. Before joining the network, users should register their vehicles to the CA server through the Internet. Users should also provide their public keys (generated on their vehicles' unique identities) to the CA for identification, and in turn, users will receive a public key of CA. We assume that CA is attack-resistant by applying IDS and access control technology.

(2) Cookies: the *Cookie* is defined as trust information in our model. It contains the feedback value of the transaction and other information. Details are shown in Table 1. The feedback value can be expressed either in a binary way (i.e., the node is rated 1 if it is satisfied with the service and 0 otherwise) or in a continuous range $[0, 1]$ to evaluate different levels of quality. *Relationship* is also an important attribute when evaluating trust. According to the relationship between the rater and the ratee (SOR, POR, or CWOR), the feedback value will be assigned different weights. Nodes extract useful information from *Cookies* to evaluate trust values toward others. *Cookies* are generated toward service provider and sent to the service provider as their credibility information. They are also stored locally in case that they may contact with the same node in the future so that they can be used as direct evidence.

(3) Relationship Management (RM): RM is module first proposed in [6]. A node's relationships with other nodes are recorded in Relationship Management. RM aims to automatically establish relationships with another node it contacts with. For example, if the vehicle B is produced by the same manufacturer as vehicle A, the *Relationship Management* of A will establish a POR with B and record this relationship in local storage. When new *Cookies* come, RM will establish the relationship shared between the ratee and the rater by looking up local relationship list.

(4) Local Trust Management (LTM): in RTM, the trust information is stored in the ratee's local storage. However, to show its credibility, the ratee has to deliver its *Cookies* to the rater to calculate the trustworthiness in the rater's LTM. If the rater has never interacted with the ratee, the trustworthiness only relies on the ratee's *Cookies*. If the rater has stored the *Cookies* generated during past interactions with the ratee, the LTM of the rater has to first calculate the trustworthiness using the rater's *Cookies* as direct experience and then calculate the trustworthiness using the ratee's *Cookies* as indirect opinion. In the end, the weighted sum of the direct experience and the indirect opinion will be the final trust value of the ratee.

4.2. Trust Validation. In a Ratee-based Trust Management system, the primary issue is that when the ratee manages its

Table 1: Attributes of *Cookies*.

Rater ID	Unique identity of the rater
Ratee ID	Unique identity of the ratee
Relationship	The relationship between the rater and the ratee
Time	When the *Cookie* is generated and when the *Cookie* will become invalid over a certain period of time
Transaction number	The number of transactions between two nodes
Feedback value	The quality of the transaction

own reputation, it is very easy for the ratee to lie or manipulate the evidence. In this case, if cookies are signed by the CA and stored by the ratee, any time vehicle B wants to evaluate the trustworthiness of vehicle A, B can request A's signed cookies, and A can share only those with positive feedback. To address this issue, we introduce asymmetric cryptography to prevent the trust information from being modified or deleted.

The trust information of a ratee (take vehicle A as an example) can be considered as a set of *Cookies* accumulated during past interactions. Whenever a single *Cookie* of the interaction between A and the rater (take vehicle B as an example) is generated, it will be uploaded to the CA server and included into the *Cookie set* of vehicle A according to vehicle A's ID. At the same time, any *Cookie* that exceeds the time limit will be excluded.

If vehicle A connects the Internet, the *Cookie set* will be updated by replacing the whole set with that from the CA server. To ensure the integrality of the *Cookie set*, the digest of the set is calculated and signed by the CA server. Therefore, vehicle B can validate the whole set of *Cookies* of vehicle A by using the CA's public key and checking the digest. If any deceit behavior comes to light, vehicle A will be added to the blacklist of vehicle B and reported to the CA; then the message will be spread to the whole network.

4.3. Trust Model. There are some sociologic and anthropological studies proving that a large number of individuals tied to social relationships can provide far more accurate answers to complex problems than a single individual [22]. In IoV scenario, a significant number of objects move with high mobility, which produces a large amount of data so that every node in the network can benefit from the discovery of services. SIoV allows vehicles and RSUs create their own relationships with respect to their owners and use these relationships to look for demanding services. In SIoV, three typical relationships are defined: *Parental Object Relationship* (POR), *Social Object Relationship* (SOR), and *Co-Work Object Relationship* (CWOR), which has been described in [2]. Our trust model is similar to the subjective model proposed by Nitti et al. [7] for SIoT. But their subjective model is not suitable to be applied in SIoV directly. In our trust model, we change the storage from rater-based to ratee-based and modify some factors to adjust the ephemeral nature of vehicular networks. We identify four major factors to estimate trust value described as follows:

Table 2: Parameters for different relationships.

Social Object Relationship (SOR)	0.5
Parental Object Relationship (POR)	0.6
Co-Work Object Relationship (CWOR)	0.8

(1) Cookies number: the number of *Cookies* received by node o_i, indicated by N_i. In addition, a node o_i is not allowed to receive more than one *Cookie* from node o_j, so it will keep the latest *Cookie* delivered by o_j. This can prevent N_i from unlimited growth, and higher N_i means more credible node o_i.

(2) Relationship factor R_{ij}: R_{ij} indicates a measure of the relationship between node o_i and node o_j, which is a unique characteristic of the SIoT. This factor is related to the relationship value and the number of interactions between two nodes. We sign different values to each relationship, respectively, as shown in Table 2. The basic idea of *Relationship Factor* is that as interaction number grows, the closer friends are more reliable. So we define that R_{ij} is calculated as follows:

$$R_{ij} = -\frac{1}{e^{\varepsilon \times N_{\text{interaction}}}} + 1, \tag{1}$$

where ε is the relationship value according to Table 2 and $N_{\text{interaction}}$ is interaction number between o_i and o_j. As interaction number grows, the value of R_{ij} will infinitely approach 1 and the growth rate will become slower.

(3) Object type: in our model, we only consider two types of objects, OBUs and RSUs. Compared with OBUs, RSUs are static and the quantity is smaller. Furthermore, it is assumed that RSUs are more credible than OBUs, because of the general idea that RSUs are under strict control. So we assign different weights to OBUs and RSUs as 0.5 and 0.8, respectively, when counting trust.

(4) Centrality: the *Centrality* (Central_{ij}) of node o_i represents how much node o_j is central to node o_i. This factor helps prevent malicious nodes that build up many relationships to raise their trust value. The definition of Central_{ij} is as follows:

$$\text{Central}_{ij} = \frac{|Q_{ij}|}{(S_i - 1)}. \tag{2}$$

The general idea is that if two nodes have few friends in common, the impact of o_j to o_i is little, even though o_j has a lot of friends.

4.4. Ratee-Based Trust Management. Different from most existing trust models, our model is ratee-based, where trust information about the quality of a transaction *(Cookies)* from the rater is stored in both the local storage of the ratee and the rater. This happens to cope with sparsity because *Cookies* from others are easy to accumulate. If the rater has never

interacted with the ratee, the trustworthiness only relies on the ratee's *Cookies* (direct experience). If the rater has stored the *Cookies* generated during past interactions with the ratee, the rater has to first compute the trustworthiness using the rater's *Cookies* as direct experience and then compute the trustworthiness using the ratee's *Cookies* as indirect opinion. In the end, the weighted sum of the direct experience and the indirect opinion will be the final trust value of the ratee. When an interaction between nodes o_i and o_j happens, for example, o_i is the requester and o_j is the provider, o_j delivers the set of *Cookies* to o_i to show its credibility. The trustworthiness of o_i toward o_j (T_{ij}) is computed as follows:

$$T_{ij} = (1 - \alpha - \beta)\,\text{Central}_{ij} + \alpha\varphi_{ij}^{\text{dir}} + \beta\phi_{ij}^{\text{ind}}, \tag{3}$$

where $\varphi_{ij}^{\text{dir}}$ and ϕ_{ij}^{ind} are direct experience toward the provider and indirect opinion from others, respectively, and α and β are the weights assigned to $\varphi_{ij}^{\text{dir}}$ and $\beta\phi_{ij}^{\text{ind}}$, respectively. The computation of $\varphi_{ij}^{\text{dir}}$ is based on the *Cookies* that are sent to o_j as feedback and are stored in o_i locally. We assume that the set of *Cookies* are valid (which means they are within a certain period of time), and $\varphi_{ij}^{\text{dir}}$ is computed as follows:

$$\varphi_{ij}^{\text{dir}} = \frac{\log(n+1)}{1+\log(n+1)} \times \sum_{k=1}^{n} f_{ij}^{k} + \frac{R_{ij}}{1+\log(n+1)}, \tag{4}$$

where f_{ij}^{k} represents the kth feedback value from o_i to o_j. The algorithm for direct trust is shown in Algorithm 1.

Indirect trust ϕ_{ij}^{ind} is computed based on the *Cookies* received from o_j. The raters of each *Cookie* can be regarded as recommenders to o_i. So the direct trust value from o_i toward each recommender should be firstly calculated as Algorithm 1. Secondly, the direct trust value from recommenders toward o_j is computed, but the algorithm is not the same as Algorithm 1, because the relationship between recommenders and o_j should not be considered in case of the bias of close friends. ϕ_{ij}^{ind} is computed as follows:

$$\phi_{ij}^{\text{ind}} = \frac{\sum_{k=1}^{n}\left(\varphi_{kj}^{\text{dir}}\right)}{\sum_{k=1}^{n}\left(\varphi_{ik}^{\text{dir}}\right)}. \tag{5}$$

The algorithm for indirect trust is shown in Algorithm 2.

Parameters α and β aim to tune the tradeoff between direct experience and indirect opinion when counting T_{ij}. In our model, we allow the weight ratios α and β to be adjusted dynamically by users in response to changing network conditions.

4.5. Cost Analysis. Trust management comes at the expenses of an increase in the network traffic and computational burden caused by the exchange of feedback information and the evaluation of trustworthiness, respectively. In RTM, a node evaluates its trust toward other nodes upon interacting with another node. Each node always keeps its *Cookies* updated by storing the latest *Cookie* delivered by another node and invalidating other *Cookies* sent by the same node. Therefore, the storage cost per node is $O(N_v)$ where N_v is the number of vehicles in an urban area.

The evaluation of trust consists of the evaluation of direct experience and indirect opinion. The evaluation of direct experience only uses the *Cookies* stored locally, so the computation time of each transaction costs $O(N_{\text{cl}})$ where N_{cl} is the number of the local *Cookies*. As for the evaluation of indirect opinion, the trust toward the recommender and the recommender toward the ratee should be calculated at each iteration, so the computation time of each transaction costs $O(N_{\text{cr}}^2)$ where cr is the number of the received *Cookies*. In practice N_{cl} and N_{cr} are smaller than N_v because a node leaves no more than one *Cookie* in another node.

4.6. Privacy. Privacy is an important concern in vehicular networks. In this scenario, the transactions of service information may reveal a vehicle owner's identity, which may allow a possibly malicious party to cause damage to the owner.

The need for privacy in RTM is that the *Cookies* should not allow for their sender to be identified, and two or more *Cookies* generated by the same node should be difficult to link to each other. During the last decade, many *pseudonym*-based mechanisms have been proposed to enhance the privacy and security of the VANETs. Calandriello et al. [23] propose an efficient and robust pseudonymous mechanism for VANETs, which can be applied in our trust system to protect users' privacy. In the proposed mechanism, it is assumed that each node has a long-term, unique identity and cryptographic keys associated with their long-term identities, managed by the CA which is the same as the CA described in Section 4.1. Each node generates its own pseudonyms, and at each transaction, it switches to a new signing key and the corresponding public key, every π seconds. Only messages signed with the same public key can be linked to each other. This is the core idea behind pseudonym schemes, and the authors propose a number of optimizations to reduce the higher transmission and processing cost caused by self-generation of pseudonyms.

5. Experimental Evaluation

In this section, the performance of the proposed RTM scheme is evaluated and the experimental results are presented with a detailed analysis.

5.1. Simulation Setup. Due to the dearth of platforms available for simulating trust management in vehicular networks, we built a V2V/V2I trust simulator as an extension to the open source VANET simulator called VANETsim [24]. VANETsim aims to investigate application-level privacy and security implications in vehicular communications. It has an interface to import maps from the *OpenStreetMap* project [25], so the simulation of traffic on real road networks is supported. The map we choose in our experiment is Berlin city, and the screenshot of the scenario is shown in Figure 3, where 1000 vehicles and 100 RSUs are simulated and shown as black dots and green dots, respectively. The vehicles are generated randomly with the properties listed in Table 3, and RSUs are distributed evenly beside the lanes. Parameters α and β are set to 0.8 and 0.2, respectively, against

Input: the set of *Cookies* C^i, the number of *Cookies* n,
relationship value ε_{ij}
Output: direct trust value $\varphi_{ij}^{\text{dir}}$
(1) $\varphi_{ij}^{\text{dir}} = 0$;
(2) sumFeedback = 0;
(3) $R_{ij} = -1/e^{\varepsilon_{ij} \times n} + 1$;
(4) **for** $j \leftarrow 1$ **to** n **do**
(5) sumFeedback+ = $C_j^i \cdot$ feedbackValue;
(6) $\varphi_{ij}^{\text{dir}} = \log(n+1)/(1+\log(n+1)) \times \text{sumFeedback} + R_{ij}/(1+\log(n+1))$;

Algorithm 1: Direct trust algorithm.

Input: the set of *Cookies* C^j, the number of *Cookies* n,
relationship value ε, relation list L_i of o_i
Output: indirect trust value ϕ_{ij}^{indir}
(1) $\phi_{ij}^{\text{indir}} = 0$;
(2) $\text{sumTrust}_{ik} = 0$;
(3) $\text{sumTrust}_{kj} = 0$;
(4) $\text{sumFeedback}_{kj} = 0$;
(5) **for** $i \leftarrow 1$ **to** n **do**
(6) *define* k *is the rater of* C_i^j;
(7) **if** $C_i^j \cdot$ raterID in L_i **then**
(8) *compute* $\varphi_{ik}^{\text{dir}}$ *as Algorithm 1*;
(9) **else**
(10) *assign a certain value to* $\varphi_{ik}^{\text{dir}}$
(11) $\text{sumTrust}_{ik}+ = \varphi_{ik}^{\text{dir}}$;
(12) $\text{sumFeedback}_{kj}+ = C_i^j \cdot$ feedbackValue;
(13) $\text{sumTrust}_{kj} = (\log(n+1) \times \text{sumFeedback}_{kj})/(1+\log(n+1))$;
(14) $\phi_{ij}^{\text{indir}} = \text{sumTrust}_{kj}/\text{sumTrust}_{ik}$;

Algorithm 2: Indirect trust algorithm.

Table 3: Properties of vehicles.

Min. speed, km/h	100
Max. speed, km/h	200
Acceleration rate, cm/s^2	300
Braking rate, cm/s^2	800
Communication range, m	100
Vehicle length, cm	600
Communication interval, ms	1000

bad-mouthing attack. At the start of the simulation, 100 of the vehicles are randomly selected to have a certain relationship with each other. Because of the limit of the platform, CA server is not considered in our simulation, so the experiment is based on the belief that the *Cookies* will not be tampered.

5.2. Performance Matrices. The main advantage of RTM is the capability with sparsity. Because of the distributed storage of *Cookies*, every piece of interaction information can be used as trust element to estimate trustworthiness. New comers can instantly get services from the network and

Figure 3: The simulation of the scenario of Berlin city with 1000 vehicles and 100 RSUs.

establish trust with the provider based on their *Cookies*. We run several simulations to evaluate our system compared with the rater-based trust management, and detailed results and analysis regarding interaction growth, success rate, and system computation time will be presented.

5.2.1. Transaction Number Growth. In the simulation, we record the number of interactions between vehicles for 10

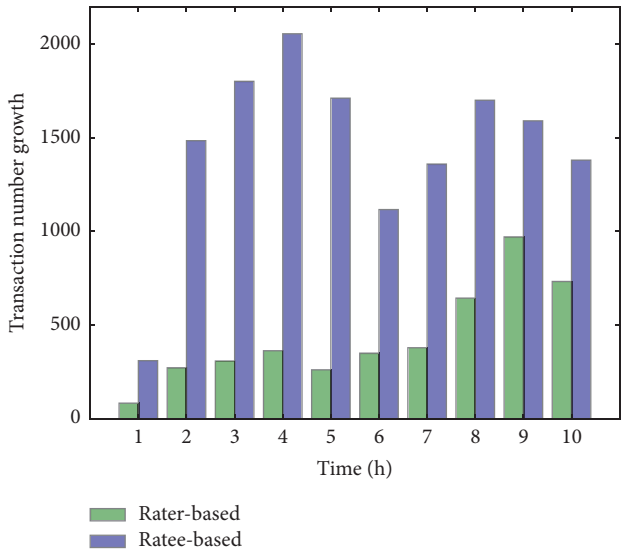

Figure 4: Transaction number growth in each hour.

hours, and the interaction growth in each hour of both methods is calculated. The results are depicted in Figure 4. In the first hour, the increase of transaction number of both methods is slow and rater-based method is slower. This is because, in the initial state of the network, few nodes are related and the interaction information needs time to accumulate to estimate trust. During the rest of the time, the transaction number of ratee-based method grows fast and peaks at more than 2000 transactions in the 4th hour, while merely less than 400 transactions' growth is observed in the rater-based method. It is after the 7th hour that the growth of the rater-based method began to accelerate, but the number is still about 500 less than that of the ratee-based method.

Experimental results illustrate that, in ratee-based method, every *Cookie* can be used to estimate trust instantly after generation. With more interactions, the accumulation of *Cookies* will accelerate. In contrast, rater-based method cannot guarantee that every piece of information produced in interactions will be used in the next time, so the interaction number grows slower than the ratee-based method. After a period of time, the growth of transaction number will fluctuate in a balanced state.

5.2.2. Transaction Success Rate. We define the malicious nodes as nodes that provide misleading information when providing services and inaccurate feedback *Cookies* when rating services. In this experiment, the percentage of malicious nodes (denoted by mp) is set to 10%, 20%, 30%, and 40%, respectively. The purpose of this experiment is to analyze how transaction success rate of our method grows at different malicious scenarios. Figure 5 shows the results.

Experimental results demonstrate that the ratee-based method has a faster convergence and a higher success rate after convergence. In Figure 5(a), when mp = 10% the time of convergence of the ratee-based method is only half an hour, while in the rater-based method, the time is more than 6 hours. We note that as mp grows, the success rate of both ratee-based and rater-based methods decreases since the estimation of trust value is profoundly influenced by malicious feedback. Furthermore, the ratee-based method is more sensitive to malicious nodes, because when a good node gets enough feedback from malicious nodes, it is difficult for the node to get more *Cookies* from others to recover its reputation until bad *Cookies* expire.

5.2.3. System Computation Time. The system computation time includes cookie validation time and trustworthiness calculation time. The CA server is not needed in real time, so the vehicle-CA interaction time is not considered. In this experiment, CanaKit Raspberry PI 3 is used to simulate the vehicle. This Raspberry PI 3 contains an ARMv8 quad-core Cortex-A53 CPU with 1.2 GHz processing speed and 1 GB RAM. It also has built-in Bluetooth and Wi-Fi ports for wireless communication. The validation program and trustworthiness computation algorithms are implemented by python 2.7. Each *Cookie* is about 10 bytes, and we test the number of *Cookies* from 10 to 100.

Figure 6 demonstrates the computation time under different number of *Cookies*. The main focus is to understand how long it will take to validate *Cookies* and compute trustworthiness. We found a linear relationship for computation time by instrumenting the number of *Cookies* and the time cost. Notably, the total computation time is still less than 0.1 s when the *Cookie* number reaches 100, which meets the demand of vehicular networks.

6. Conclusions

In this paper, we focus on the trust issue in the social IoV by proposing a Ratee-based Trust Management (RTM) system, where each node stores its own reputation information rated by others during past transactions. In RTM, each node estimates the service provider's trust value based on the social relationship with the provider and the provider's *Cookies*, which are generated during past interactions. By establishing the social relationship shared between the requester and the provider, the trustworthiness of the provider is more accurate. To prevent the trust information from being modified or deleted by the ratee, we introduce the CA server and public-key cryptography. Every trust evidence *(Cookie)* of each vehicle will be packed up and signed by the CA, and the new *Cookie set* will replace all the *Cookies* in the vehicle when it connects to the CA. Additionally, we evaluated the performance of our system by implementing a trust simulator as an extension to an open source VANET simulator. Experimental results demonstrate that, compared with the rater-based method, the proposed ratee-based method has a faster convergence and higher transaction success rate. We also used Raspberry PIs to measure computation time when calculating trustworthiness, and the result showed a linear relationship between the time cost and the number of *Cookies*.

As for future work, our proposed scheme can be enhanced by introducing intrusion detect technologies to prevent the network from external attacks. Also, the privacy issue in a Ratee-based Trust Management system remains to be well investigated in the future.

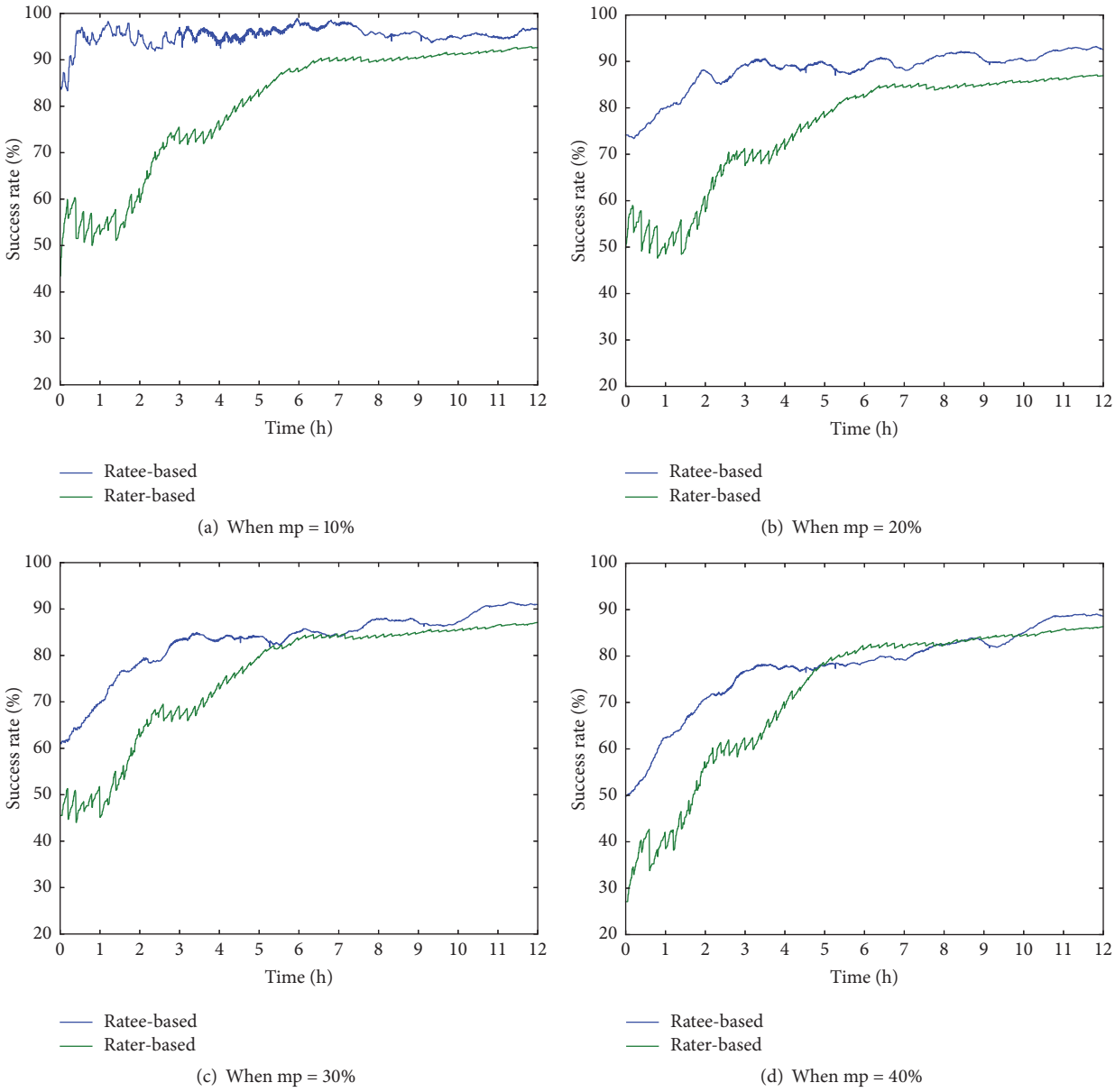

Figure 5: Success rate at different malicious percentage.

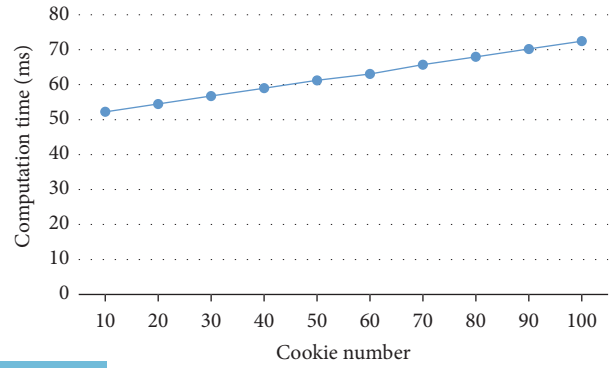

Figure 6: Computation time with *Cookies* at different numbers.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the National Science Foundation of China under Grants nos. 61272010, 61572514, and 61379117.

References

[1] F. Gai, J. Zhang, P. Zhu, and X. Jiang, "Ratee-based trust management system for internet of vehicles," in *Proceedings of the International Conference on Wireless Algorithms, Systems, and Applications*, pp. 344–355, Springer, 2017.

[2] M. Nitti, R. Girau, A. Floris, and L. Atzori, "On adding the social dimension to the Internet of Vehicles: Friendship and middleware," in *Proceedings of the 2014 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom 2014*, pp. 134–138, May 2014.

[3] A. Dua, N. Kumar, and S. Bawa, "A systematic review on routing protocols for Vehicular Ad Hoc Networks," *Vehicular Communications*, vol. 1, no. 1, pp. 33–52, 2014.

[4] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, "An overview of internet of vehicles," *Wireless Communication Over Zigbee for Automotive Inclination Measurement China Communications*, vol. 11, no. 10, pp. 1–15, 2014.

[5] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: from intelligent grid to autonomous cars and vehicular clouds," in *Proceedings of the IEEE World Forum on Internet of Things (WF-IoT '14)*, pp. 241–246, March 2014.

[6] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (SIoT)—when social networks meet the internet of things: concept, architecture and network characterization," *Computer Networks*, vol. 56, no. 16, pp. 3594–3608, 2012.

[7] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social internet of things," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 5, pp. 1253–1266, 2014.

[8] K. M. Alam, M. Saini, and A. El Saddik, "Toward social internet of vehicles: concept, architecture, and applications," *IEEE Access*, vol. 3, pp. 343–357, 2015.

[9] L. Atzori, A. Iera, and G. Morabito, "SIoT: giving a social structure to the internet of things," *IEEE Communications Letters*, vol. 15, no. 11, pp. 1193–1195, 2011.

[10] G. Karagiannis, O. Altintas, E. Ekici et al., "Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 584–616, 2011.

[11] S. Buchegger and J. Y. Le Boudec, "Performance analysis of the confidant protocol," in *Proceedings of the ACM Interational Symposium on Mobile Ad Hoc NETWORKING and Computing, MOBIHOC 2002*, pp. 226–236, Lausanne, Switzerland, June 2002.

[12] P. Michiardi and R. Molva, *Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks*, vol. 100, IFIP — the International Federation for Information Processing, 2002.

[13] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in *Proceedings of the 2006 3rd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, MobiQuitous*, pp. 1–8, July 2006.

[14] S. Buchegger, "A Robust Reputation System for Mobile Ad-Hoc Networks," Tech. Rep., P2pecon, 2003.

[15] J. Zhang, "A survey on trust management for vanets," in *Proceedings of the Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on. IEEE*, pp. 105–112, 2011.

[16] F. Kargl, P. Papadimitratos, L. Buttyan et al., "Secure vehicular communication systems: implementation, performance, and research challenges," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 110–118, 2008.

[17] D. Huang, X. Hong, and M. Gerla, "Situation-Aware Trust architecture for vehicular networks," *IEEE Communications Magazine*, vol. 48, no. 11, pp. 128–135, 2010.

[18] W. Li and H. Song, "ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1–10, 2016.

[19] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Intelligent Agents in Mobile Vehicular Ad-Hoc Networks: Leveraging Trust Modeling Based on Direct Experience with Incentives for Honesty," in *Proceedings of the 2010 IEEE/ACM International Conference on Web Intelligence-Intelligent Agent Technology (WI-IAT)*, pp. 243–247, Toronto, AB, Canada, August 2010.

[20] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," *ACM Computing Surveys*, vol. 42, no. 1, article 1, 2009.

[21] J. R. Douceur, "The sybil attack," in *Proceedings of the International Workshop on Peer-to-Peer Systems*, pp. 251–260, Springer, 2002.

[22] M. P. Silverman, "The wisdom of crowds," *American Journal of Physics*, vol. 75, no. 2, pp. 190–192, 2007.

[23] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in *In Proceedings of the Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks, VANET'07*, pp. 19–28, ACM, New York, NY, USA, 2007.

[24] A. Tomandl, D. Herrmann, K. Fuchs, H. Federrath, and F. Scheuer, "VANETsim: An open source simulator for security and privacy concepts in VANETs," in *Proceedings of the 2014 International Conference on High Performance Computing & Simulation (HPCS)*, pp. 543–550, Bologna, Italy, July 2014.

[25] M. Haklay and P. Weber, "Openstreetmap: user-generated street maps," *IEEE Pervasive Computing*, vol. 7, no. 4, pp. 12–18, 2008.