Hindawi Publishing Corporation
Mobile Information Systems
Volume 2016, Article ID 7628231, 15 pages
http://dx.doi.org/10.1155/2016/7628231

Research Article

LSOT: A Lightweight Self-Organized Trust Model in VANETs

Zhiquan Liu,[1] Jianfeng Ma,[1,2] Zhongyuan Jiang,[2] Hui Zhu,[2] and Yinbin Miao[3]

[1]*School of Computer Science and Technology, Xidian University, Xi'an 710071, China*
[2]*School of Cyber Engineering, Xidian University, Xi'an 710071, China*
[3]*School of Telecommunication Engineering, Xidian University, Xi'an 710071, China*

Correspondence should be addressed to Jianfeng Ma; jfma@mail.xidian.edu.cn

Received 23 June 2016; Accepted 13 November 2016

Academic Editor: Elio Masciari

With the advances in automobile industry and wireless communication technology, Vehicular Ad hoc Networks (VANETs) have attracted the attention of a large number of researchers. Trust management plays an important role in VANETs. However, it is still at the preliminary stage and the existing trust models cannot entirely conform to the characteristics of VANETs. This work proposes a novel Lightweight Self-Organized Trust (LSOT) model which contains trust certificate-based and recommendation-based trust evaluations. Both the supernodes and trusted third parties are not needed in our model. In addition, we comprehensively consider three factor weights to ease the collusion attack in trust certificate-based trust evaluation, and we utilize the testing interaction method to build and maintain the trust network and propose a maximum local trust (MLT) algorithm to identify trustworthy recommenders in recommendation-based trust evaluation. Furthermore, a fully distributed VANET scenario is deployed based on the famous Advogato dataset and a series of simulations and analysis are conducted. The results illustrate that our LSOT model significantly outperforms the excellent experience-based trust (EBT) and Lightweight Cross-domain Trust (LCT) models in terms of evaluation performance and robustness against the collusion attack.

1. Introduction

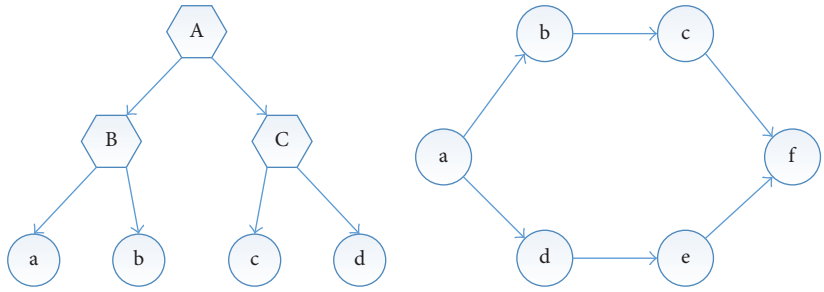
Nowadays, an increasing number of vehicles are being equipped with position and wireless communication devices, which forms an independent research area known as VANETs [1, 2]. Furthermore, VANETs have become one of the most prominent branches of Mobile Ad hoc Networks (MANETs) as they contribute to the increased road safety and passenger comfort [3–5].

In VANETs, the participating nodes (i.e., vehicles) can interact and cooperate with each other by exchanging messages through nearby roadside units (i.e., vehicle to infrastructure) and intermediate vehicles (i.e., vehicle to vehicle) [6]. However, due to the characteristics of VANETs, namely, being large, open, distributed, highly dynamic, and sparse, they are vulnerable to some malicious behaviors and attacks [7].

Traditional cryptography and digital signature technologies mainly focus on ensuring the verifiability, integrity, and nonrepudiation of messages among nodes and little concerns have been placed on evaluating the quality of messages and nodes to deal with unreal information from malicious nodes which may compromise VANETs [13, 14]. In fact, authenticated nodes may also send out unreal information or collude with others to cheat honest nodes for their own sake [15, 16].

Trust management plays a significant role in VANETs as it enables each node to evaluate the trust values of other nodes before acting on a message from other nodes for the purpose of avoiding the dire consequences caused by the unreal messages from malicious nodes [17]. However, recently only a few trust models in VANETs have been proposed [8, 9, 11, 18–22] and they can be roughly divided into two categories, namely, infrastructure-based and self-organized models [7, 23].

Infrastructure-based trust models (as shown in Figure 1(a)) [8, 9, 18, 19] usually include the hierarchical Certificate Authorities (CAs) which are supposed to be totally



(a) Infrastructure-based models (b) Self-organized models

Figure 1: Classic trust models in VANETs (where A~C denote CAs and a~f represent vehicles).

trusted and able to satisfy a variety of security needs, such as authentication, integrity, nonrepudiation, and privacy. However, this kind of trust models requires too strong assumption. For example, in these models, the CAs must be totally trusted and online at all the time, and every vehicle must be able to access to the CAs at any time, while, in reality, the CAs may break down or even collude with some malicious vehicles to cheat other honest ones, and the vehicles may not be able to connect to the CAs where the roadside units are not available (e.g., outside the city).

Since the self-organized models are more applicable to the distributed and highly dynamic environment of VANETs, most of the recent trust models are built in this manner (as shown in Figure 1(b)) [11, 20–22]. In these models, the CAs are not guaranteed at all the time and each node evaluates the trust value of target node based on the local knowledge obtained from its past experiences and the recommendations of neighbor nodes during a short period of time. Though a few self-organized trust models have been proposed, there still exist the following drawbacks in them.

(a) Due to the high dynamic characteristic, VANETs are indeed temporary networks and the connections among nodes are short-lived. In most cases, a node will not interact with the other same nodes more than once [24]. As a result, *the self's past experiences are usually not available for trust evaluation*.

(b) Most of the messages in VANETs are time-critical (e.g., the reports about traffic jams or accidents) and the nodes need to evaluate their trust quickly and decide whether to act on them or not, while *collecting the trust recommendations requires large amounts of time and bandwidth resources* [12], which does not conform well to the natures of VANETs.

(c) Though trust management can effectively detect the malicious nodes and false messages and promote the node collaboration, the trust model self may become the target of attacks, such as the notorious collusion attack which is an open problem in the area of trust and reputation system [14], while *the existing self-organized trust schemes rarely consider the robustness against the collusion attack*.

To the best of our knowledge, there is no existing distinguished trust model for VANETs that has overcome all the above limitations. This is just the motivation of our work. In this paper, we introduce the *trust certificate* [10, 12] and *testing interaction* [25, 26] and propose a novel LSOT model for VANETs. The major characteristics and contributions of our proposed model are summarized as follows.

(a) Our LSOT Model Is Built in a Lightweight and Fully Distributed Manner. In our proposed model, the nodes are self-organized and both the supernodes (e.g., the nodes with special roles) and trusted third parties (e.g., CAs) are not needed. Moreover, as our LSOT model aggregates both trust certificate-based and recommendation-based trust evaluations, the evaluations in our model can be made quickly and reach an excellent performance in a lightweight manner.

(b) Our LSOT Model Has High Evaluation Performance. To demonstrate the performance of our proposed model, we deploy a VANET scenario based on the noted Advogato dataset (http://konect.uni-koblenz.de/networks/advogato) and conduct a series of simulations and analysis. The results demonstrate that our proposed model significantly outperforms the excellent EBT model [25] and LCT model [12] in terms of the evaluation performance.

(c) Our LSOT Model Has Strong Robustness against the Collusion Attack. In our LSOT model, we adopt the testing interaction method to build and maintain the trust recommendation network and combine trust certificate-based and recommendation-based trust evaluations. Thus our proposed model has stronger robustness against the collusion attack than LCT model, which has been verified by the simulations and analysis.

The rest of this paper is organized as follows. Section 2 includes some related work and its limitations. Section 3 demonstrates the motivation and general evaluation procedure of our LSOT model, and the trust certificate-based and recommendation-based trust evaluations are detailed in Sections 4 and 5, respectively. Afterwards, Section 6 introduces the aggregation evaluation method. Comprehensive simulations and analysis are presented in Section 7 and Section 8 concludes this paper.

2. Related Work

In recent years, a great deal of research work for VANETs has been done by utilizing digital signature and cryptography technologies. Security and privacy have been widely concerned, and the architectures, challenges, requirements, attacks, and solutions in VANETs have been analyzed by several researchers [13, 27–30]. However, these schemes mainly pay attention to ensuring the verifiability, integrity, and nonrepudiation of messages among nodes and little concerns have been placed on evaluating the quality of messages and nodes. In actual fact, an authenticated node may also send out unreal messages for its own sake and others cannot perceive them in advance.

Trust management has been proved to be a very useful solution for the mobile distributed environments as it enables each node to evaluate the trust values of others in advance so as to avoid interacting with malicious or selfish nodes. A large number of trust models have been proposed for MANETs [31], Wireless Sensor Networks (WSNs) [32–34], and Mobile Peer to Peer networks (MP2Ps) [35]. However, these trust models are not suitable to VANETs due to the unique characteristics and requirements in this field.

Currently, trust management in VANETs is still at a preliminary stage and only a few trust models have been proposed. These trust models can mainly be classified into two categories, namely, infrastructure-based and self-organized models.

In the infrastructure-based schemes, CAs are tasked with maintaining the trust scores of vehicles. Wu et al. [18] proposed a Roadside-unit Aided Trust Establishment (RATE) model for VANETs. This model contains three properties, namely, infrastructure-based architecture, data-centric pattern, and integration of observation and feedback. Park et al. [8] introduced a simple Long-Term Reputation (LTR) scheme based on the fact that plenty of vehicles have predefined constant daily trajectories. In this model, roadside units monitor the daily behaviors of vehicles and update their reputation values. To ensure the freshness of reputation scores, the users have to query the roadside units frequently. Gómez Mármol and Martínez Pérez [19] surveyed the deficiency of existing trust models in VANETs and suggested a set of design requirements for trust schemes which are specifically suitable to VANETs. Furthermore, they also presented an original Trust and Reputation Infrastructure-based Proposal (TRIP) from a behavioral perspective, instead of an identity-based one. Li et al. [9] introduced a Reputation-based Global Trust Establishment (RGTE) scheme in which the reputation management center is responsible for collecting the trust information from all legal nodes and calculating the reputation scores of nodes.

As we mentioned earlier, the infrastructure-based schemes require too strong assumptions and may lead to some issues, such as single point of failure and high maintenance cost. Thus most of the recent trust models for VANETs are built in a self-organized manner. Yang [20] proposed a novel Trust and Reputation Management Framework based on the Similarity (TRMFS) between messages and between vehicles. They also presented a similarity mining technique to identify similarity and an updating algorithm to calculate the reputation values. Bamberger et al. [21] introduced an Inter-vehicular Communication trust model based on Belief Theory (ICBT). This model mainly focuses on the direct experiences among vehicles and utilizes binary error and erasure channel to make a decision based on the collected data. Hong et al. [22] noticed that VANETs face lots of situations and quickly change among different situations; then they described a novel Situation-Aware Trust (SAT) model which includes three important components. Huang et al. [11] absorbed the Information Cascading and Oversampling (ICO) into VANETs and proposed a novel voting scheme, in which each vote has different weight based on the distance between sender and event.

Though the above schemes provide many brilliant ideas, there exist several limitations as we analyzed earlier. In our previous work [12], we improved the classic Certified Reputation (CR) model [10] and proposed a LCT model for the mobile distributed environment. In this model, the trust certificates are adopted as they can be carried by trustees and contribute to establishing the trust relationships in highly dynamic environment in a fast and lightweight manner. However, this model is intuitively vulnerable to the collusion attack. In addition, to tackle the sparse issue of VANETs, Minhas et al. [25] introduced a novel EBT scheme, in which the vehicles send the testing requests to each other and interactively compute the trust values of others based on the quality of responses. By this way, a trust network can be built and updated dynamically. However, the supernodes with special roles are needed in this model; thus in essence this model is not built in a fully self-organized way.

Aiming at building a lightweight trust model for VANETs in a fully self-organized way as well as overcoming the limitations of aforementioned schemes, we propose a novel LSOT model in this paper and the intuitive comparisons with some other trust models are illustrated in Table 1.

3. The Framework of Our LSOT Model

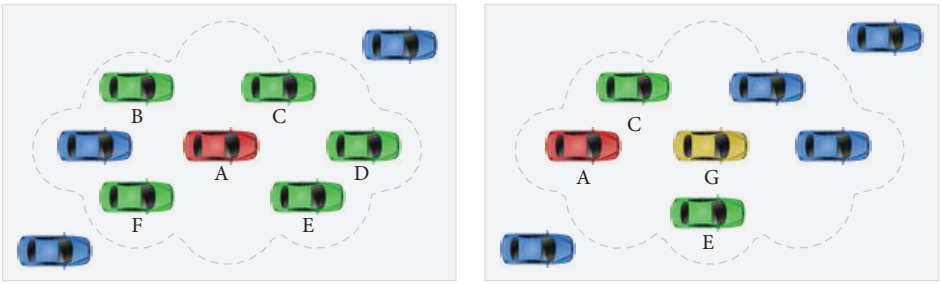
In this section, we first show the motivation of our work with a fully self-organized VANET scenario. Afterwards, we introduce the general evaluation procedure in our proposed model through a simple example.

3.1. The Motivation of Our Work. Before introducing our LSOT model, we first illustrate our motivation with the following VANET scenario (as demonstrated in Figure 2). In the past interactions (as shown in Figure 2(a)), the vehicle A interacted with several nearby vehicles (e.g., B~F) and accumulated certain trust level. In a potential interaction (as shown in Figure 2(b)), A and its new neighbors (e.g., G) are strange to each other. Due to the highly dynamic feature of VANETs, the majority of previous interaction partners of A (e.g., B, D, and F) are far from G and there exists no reliable trust path between them. So G can merely collect the trust information about A from a few previous interaction partners of A (e.g., C and E; in fact they may not exist) and most of previous trust information of A (e.g., with B, D, and F) has to be ignored when building the new trust relationships between

Table 1: Intuitive comparisons between our LSOT model and some other trust models in VANETs.

Trust models	Architecture	Trust certificate	Recommendation	Cost	Robustness
LTR [8]	Infrastructure-based	×	×	High	—
RGTE [9]	Infrastructure-based	×	×	High	—
EBT [10]	Self-organized with supernodes	×	√	Midterm	—
ICO [11]	Fully self-organized	×	×	Low	Weak
LCT [12]	Fully self-organized	√	×	Low	Weak
LSOT	Fully self-organized	√	√	Low	Strong

"√": support; "×": nonsupport; "—": without consideration.



(a) Past interactions (b) Potential interaction

Figure 2: Fully self-organized VANET scenario (where A~G denote vehicles).

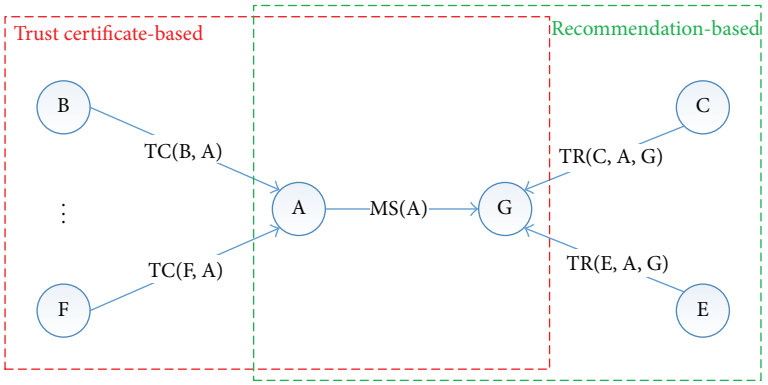


Figure 3: An example of our LSOT scheme (where A~G denote vehicles).

A and G. As a result, with the high-speed movement of A, its trust information is mostly discarded and rebuilt again and again. It is distinctly unreasonable and is just the motivation of this work. How to utilize the previous trust information to quickly build the new trust relationships is the key focus of this paper.

3.2. The Evaluation Procedure in Our LSOT Model. To deal with the above problem, we propose a novel LSOT model and a simple example is illustrated in Figure 3. It is assumed that previous interactions occur between A and B~F. At the end of past interactions, B~F provide A with their trust certificates (i.e., TC(B, A) ~ TC(F, A)) which are generated with digital signatures by B~F. Then A stores and updates the trust certificates in its local storage. In a potential interaction, A can release a message (i.e., MS(A)) which includes six parts, that is, the identification of A (ID), message type (MT), message content (MC), trust certificates (TCs), timestamp (TS), and digital signature (DS), to neighboring vehicles (e.g., G). When G receives the message, it can check the authentication and integrity of MS(A) through digital signature technology and compute the trust certificate-based trust value of A according to the trust certificates. Moreover, G can also collect the trust recommendations (e.g., TR(C, A, G) and TR(E, A, G)) about A from its trustworthy neighbors (e.g., C and E) and then derive the recommendation-based trust value of A. Afterwards, G can calculate the final trust value of A and decide whether to trust the message content or not. In the above process, A and G are defined as trustee and trustor, respectively. B~F are referred to as certifiers, and C and E are called recommenders.

Being consistent with the above example, the general evaluation procedure in our LSOT model is illustrated in Figure 4. Generally speaking, it involves four kinds of roles,

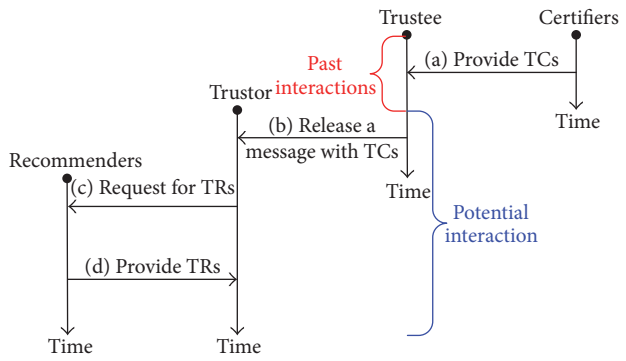


FIGURE 4: General evaluation procedure in our LSOT model.

namely, trustor (i.e., the receiver of message), trustee (i.e., the sender of message), certifier (i.e., the vehicle which provides the trust certificate), and recommender (i.e., the vehicle which has past interactions with the trustee and provides the trust recommendation to the trustor). Moreover, it mainly includes four steps: (a) At the end of past interactions, the certifiers provide their TCs to the trustee. (b) In the beginning of a potential interaction, the trustee can send out a message with TCs when needed. (c) When the trustor receives this message, it can derive the trust certificate-based trust value of the trustee based on TCs. Besides, it can also send the requests to its trustworthy neighbors for TRs. (d) The trustworthy recommenders provide TRs to the trustor, and then the trustor can obtain the recommendation-based trust value of the trustee. Afterwards, the trustor can calculate the final trust value of the trustee and decide whether to trust the message content from the trustee or not. It should be noted that we do not distinguish between the trust value of node and that of message in this paper, aiming at building a lightweight trust model for VANETs. That is to say, we utilize the trust value of a node to directly derive the trust value of message sent by the node.

In our proposed model, the trust certificates for a node are stored by itself; thus this part of trust information can be carried with the movement of node. Furthermore, the trust certificates include the digital signatures and any change to them can be easily detected [10, 12]; thus the node cannot modify the trust certificates for self-praise. Besides, the message is also attached with the digital signature; thus it cannot be tampered even relayed by other nodes. Benefiting from trust certificates, the previous trust information can be carried and utilized to conduct the trust evaluation quickly in a fully self-organized way.

4. Trust Certificate-Based Trust Evaluation

In this section, we first introduce the formal representations of trust certificate and message. Moreover, we comprehensively consider three factor weights, that is, number weight, time decay weight, and context weight, for trust certificate. Finally, we present the trust certificate-based trust calculation method in detail.

4.1. The Formal Expressions of Trust Certificate and Message. In our LSOT scheme, the trust certificate generated by certifier i for trustee j is denoted as

$$\begin{aligned} \mathrm{TC}(i,j) = {} & (\mathrm{ID}(i), \mathrm{ID}(j), \mathrm{TY}(i,j), \mathrm{RV}(i,j), \mathrm{LC}(i), \\ & \mathrm{TS}(i,j), \mathrm{DS}(i,j)), \end{aligned} \tag{1}$$

where $\mathrm{ID}(i)$ and $\mathrm{ID}(j)$ mean the identifications of certifier i and trustee j, respectively. $\mathrm{TY}(i,j)$ denotes the type of corresponding message and $\mathrm{RV}(i,j)$ represents the rating value which is a real number within the range of $[0,1]$. Larger $\mathrm{RV}(i,j)$ means higher satisfaction degree and vice versa. $\mathrm{LC}(i)$ represents the location coordinate of certifier i and $\mathrm{TS}(i,j)$ denotes the timestamp when the trust certificate is generated. $\mathrm{DS}(i,j)$ represents the digital signature. The message released by trustee j is denoted as

$$\begin{aligned} & \mathrm{MS}(j) \\ & = (\mathrm{ID}(j), \mathrm{MY}(j), \mathrm{MC}(j), \mathrm{TCs}(j), \mathrm{TS}(j), \mathrm{DS}(j)), \end{aligned} \tag{2}$$

where $\mathrm{ID}(j)$ denotes the identification of trustee j. $\mathrm{MY}(j)$ and $\mathrm{MC}(j)$ stand for the type and content of message, respectively. $\mathrm{TCs}(j)$ denotes the set of trust certificates for trustee j. $\mathrm{TS}(j)$ and $\mathrm{DS}(j)$ represent the timestamp and digital signature, respectively.

4.2. Three Factor Weights for Trust Certificate. Due to the unique feature of our LSOT scheme, the trustee may merely provide profitable trust certificates to the potential trustor or even collude with others to improve its trust value and slander its competitors (i.e., collusion attack). Besides, the trustee may first accumulate high trust value through releasing authentic but unimportant (e.g., entertainment-related) message and cheat others by issuing important (e.g., security-related) but unreal message (i.e., value imbalance attack). In order to ease these two kinds of attacks, we comprehensively consider three factor weights, that is, number weight, time decay weight, and context weight.

4.2.1. Number Weight. To balance the robustness against collusion attack and bandwidth consumption, $\mathrm{TCs}(j)$ merely consists of $N(j)$ $(N(j) \le \eta)$ most favorable trust certificates which come from diverse certifiers, where η is a system parameter which relies on current network status in terms of the collusion attack. The number weight $\mathrm{WN}(j)$ corresponding to $N(j)$ is denoted as a piecewise function [12]:

$$\mathrm{WN}(j) = \begin{cases} 0, & \text{if } N(j) < \eta, \\ 1, & \text{otherwise.} \end{cases} \tag{3}$$

If $N(j)$ is less than η, the trust certificates are considered incredible; thus $\mathrm{WN}(j)$ is set as 0. Otherwise, the trust certificates are viewed as reliable, so $\mathrm{WN}(j)$ is set as 1.

4.2.2. Time Decay Weight. As we well know, the relatively recent trust certificate is more convincing than the less recent one and the outdated trust certificate may be unreliable at

all as the behavior of trustee may change from honest to malicious in VANETs; thus the time decay weight WT(i, j) for TC(i, j) is denoted as [36]

$$\mathrm{WT}(i,j) = \begin{cases} 0, & \text{if } \mathrm{TN} - \mathrm{TS}(i,j) > \omega, \\ e^{-(\mathrm{TN}-\mathrm{TS}(i,j))/\alpha}, & \text{otherwise}, \end{cases} \tag{4}$$

where TN is the current timestamp and ω is a time window. α is a time unit which controls the speed of time decay. If the time difference between TN and TS(i, j) exceeds ω, TC(i, j) is considered unreliable; therefore WT(i, j) is set as 0. Otherwise, WT(i, j) is represented as an exponential decay function of time difference.

4.2.3. Context Weight. Last but not least, we also take the context weight into account for TC(i, j). Specifically, we consider two kinds of most important contextual properties, namely, message type and location.

(a) Message Type. As we mentioned earlier, the node may first accumulate high trust value through releasing authentic but unimportant message and then cheat the other nodes by issuing important but unreal message (i.e., value imbalance attack); thus we consider the message type similarity weight WY(i, j) for TC(i, j) as

$$\mathrm{WY}(i,j) = \begin{cases} 1, & \text{if } \rho(\mathrm{TY}(i,j)) \geq \rho(\mathrm{MY}(j)), \\ \beta, & \text{otherwise}, \end{cases} \tag{5}$$

where $\rho(*)$ is the importance function of message type and β is a constant within the range of [0, 1). If the importance of TY(i, j) is no less than that of MY(j), TC(i, j) is considered reliable and WY(i, j) is set as 1. Otherwise, TC(i, j) is regarded as not entirely credible and WY(i, j) is set as β.

(b) Location. As discussed in some related work [1, 7, 14], the location is also an important contextual property. In the view of trustor, a trust certificate from a nearby certifier is more reliable than that from a remote certifier as the latter has a higher likelihood of colluding with trustee than the former. Thus the location similarity weight WL(i, k) between trustor k and certifier i is denoted as

$$\mathrm{WL}(i,k) = \begin{cases} 0, & \text{if } \|\mathrm{LC}(i) - \mathrm{LC}(k)\| > \delta, \\ e^{-\|\mathrm{LC}(i)-\mathrm{LC}(k)\|/\lambda}, & \text{otherwise}, \end{cases} \tag{6}$$

where δ is a distance threshold and λ is a constant which controls the speed of distance decay. If the distance between certifier i and trustor k exceeds δ, TC(i, j) is viewed as unreliable; thus WL(i, k) is set as 0. Otherwise, WL(i, k) is denoted as an exponential decay function of distance.

4.3. Trust Calculation Method. Next, we detail the trust certificate-based trust calculation method. At the end of each past interaction, the certifier (e.g., i) generated a trust certificate (e.g., TC(i, j)) and sent it to trustee j. When trustee j needs to release a message MS(j), it first chooses $N(j)$ most advantageous trust certificates from its local storage based on the weighted rating value RW(i, j), which can be derived from

$$\mathrm{RW}(i,j) = \mathrm{RV}(i,j) * \mathrm{WT}(i,j) * \mathrm{WY}(i,j). \tag{7}$$

It should be noted that in VANETs the messages are usually broadcasted in a one-to-many manner; thus RW(i, j) is independent of WL(i, k) in our scheme.

When trustor k receives MS(j), it can extract $N(j)$ trust certificates and then calculate the trust certificate-based trust value CT(j, k) of MS(j) as

$$\mathrm{CT}(j,k) = \begin{cases} \dfrac{\sum_{i=1}^{\eta} \mathrm{RV}(i,j) * \mathrm{WT}(i,j) * (\mathrm{WY}(i,j) + \mathrm{WL}(i,k))}{2 * \eta}, & \text{if } N(j) = \eta, \\ \mu, & \text{otherwise}. \end{cases} \tag{8}$$

If $N(j)$ equals η, the trust certificates are viewed as reliable and CT(j, k) is calculated as the weighted average value of η ratings which come from diverse certifiers. Otherwise, the trust certificates are considered unreliable and CT(j, k) is set as a default low value μ ($0 < \mu < 1$). From (8), we can easily find that CT(j, k) falls in the range of 0~1. In actual fact, newcomer trustees may have no sufficient trust certificates, and malicious trustees may also act as newcomers and refuse to provide unfavorable trust certificates, so their trust certificate-based trust values equal μ.

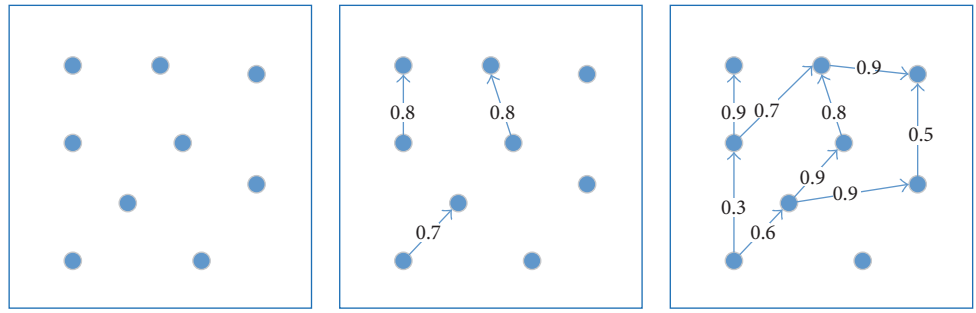
5. Recommendation-Based Trust Evaluation

In this section, we first present the formal representation of trust recommendation. Next we introduce the formation of trust network based on testing interactions. Moreover, we propose an effective MLT algorithm to identify all the trustworthy recommenders and introduce the details of recommendation-based trust calculation method.

5.1. The Formal Representation of Trust Recommendation. In our LSOT scheme, the trust recommendation on trustee j generated by recommender l for trustor k is denoted as

$$\mathrm{TR}(l,j,k) = (\mathrm{ID}(l), \mathrm{ID}(j), \mathrm{ID}(k), \mathrm{RV}(l,j,k), \mathrm{DS}(l,j,k)), \tag{9}$$

where ID(l), ID(j), and ID(k) stand for the identifications of recommender l, trustee j, and trustor k, respectively.



(a) Initial stage (b) Forming stage (c) Dynamic update stage

Figure 5: Trust network formation based on testing interactions.

RV(l, j, k) denotes the rating value and DS(l, j, k) represents the digital signature.

5.2. The Formation of Trust Network. Due to the sparse and highly dynamic characteristic, there are no sufficient or long-term trust relationships among nodes in VANETs. In order to tackle this problem, we introduce the idea of allowing nodes to send several testing requires (to which the senders have known the corresponding solutions in advance) to each other and calculate the trust values of receivers according to the accuracy and timeliness of responses. Inspired by the previous work [25, 26], we adopt and improve the classic experience-based trust evaluation scheme [37].

Let $\mathrm{TV}(s, r) \in [0, 1]$ be the trust value demonstrating the satisfaction degree of sender s to the responses of receiver r. If sender s does not receive any response from receiver r, $\mathrm{TV}(s, r)$ is set as 0. Whenever sender s receives a response from receiver r, it updates $\mathrm{TV}(s, r)$ based on the following rules:

(a) If sender s is satisfied with the new response of receiver r, $\mathrm{TV}(s, r)$ increases as

$$\mathrm{TV}(s, r) \longleftarrow \mathrm{TV}(s, r) + \phi * (1 - \mathrm{TV}(s, r)). \quad (10)$$

(b) Otherwise, $\mathrm{TV}(s, r)$ decreases as

$$\mathrm{TV}(s, r) \longleftarrow \mathrm{TV}(s, r) - \psi * \mathrm{TV}(s, r), \quad (11)$$

where ϕ and ψ are the increment and decrement factors, respectively, and their ranges are $(0, 1)$. Moreover, we set $\phi < \psi$ due to the fact that trust is difficult to build up but easy to drop off.

We can easily find that the experience-based trust is accumulated and the trust values of nodes can be updated recursively as (10) and (11). Moreover, the difficulty of the above calculations is very small and each node can evaluate the trust values of other nearby nodes easily through testing interactions; thus the trust network can be generated and dynamically updated in a lightweight manner. A simple example is shown in Figure 5.

5.3. Trust Calculation Method. In recommendation-based trust evaluation, only the ratings from trustworthy recommenders are considered. For identifying trustworthy recommenders, we propose a novel MLT algorithm (i.e., Algorithm 1) to calculate the maximum local trust values of all the recommenders in the view of trustor.

As we know, the trust network in VANETs has the highly dynamic characteristic and the reliability of trust evaluation will be very low when the trust path is too long [38]. Therefore, we consider the trust decay in our MLT algorithm. Specifically, suppose $p_0 \rightarrow p_1 \rightarrow \cdots \rightarrow p_h$ (where $p_0 = k$, $p_h = l$, and recommender l has previous interactions with trustee j) is one of the optimal trust paths from trustor k to recommender l; then the maximum local trust value $\mathrm{MT}(k, l)$ (i.e., $MT[l]$ in Algorithm 1) of recommender l from the perspective of trustor k can be obtained from [39]:

$$\mathrm{MT}(k, l) = \begin{cases} \dfrac{\prod_{m=0}^{h-1} \mathrm{TV}(p_m, p_{m+1})}{h^{\theta}}, & \text{if } h \le \mathrm{MH}, \\ 0, & \text{otherwise}, \end{cases} \quad (12)$$

where h is the hop from trustor k to recommender l and θ is a parameter which controls the speed of trust decay. If $\mathrm{MT}(k, l)$ reaches the trust threshold $\mathrm{TH}(k)$ of trustor k, recommender l is viewed as trustworthy and vice versa. Similarly, we can obtain all the elements of trustworthy recommender set $\mathrm{RS}(j, k)$ and calculate the recommendation-based trust value $\mathrm{RT}(j, k)$ of trustee j in the view of trustor k as [40]

$$\mathrm{RT}(j, k) = \begin{cases} \dfrac{\sum_{l \in \mathrm{RS}(j,k)} \mathrm{RV}(l, j, k) * \mathrm{MT}(k, l)}{\sum_{l \in \mathrm{RS}(j,k)} \mathrm{MT}(k, l)}, & \text{if } \mathrm{RS}(j, k) \neq \emptyset, \\ \nu, & \text{otherwise}. \end{cases} \quad (13)$$

If $\mathrm{RS}(j, k)$ is not empty, $\mathrm{RT}(j, k)$ is calculated as the weighted average value of ratings from all the trustworthy recommenders. Otherwise, $\mathrm{RT}(j, k)$ is set as a default low value ν $(0 < \nu < 1)$. From (10)~(13), we can find that the range of $\mathrm{RT}(j, k)$ is also 0~1.

Input: TN = (ND, TV), MH, k, θ; /*TN: Trust network based on testing interactions; ND: Node set; TV: Set of experience-based trust values among nodes; MH: Maximum allowable hop; k: Trustor; θ: Trust decay factor. */
Output: MT; /*MT: Maximum local trust array of nodes in ND from the perspective of k. */
(1) VN $\Leftarrow \emptyset$; /*VN: Visited node set which is initialized to an empty set. */
(2) MT, HP; /*HP: Hop array of nodes in ND from the perspective of k. */
(3) MT[k] $\Leftarrow$ 1, HP[k] $\Leftarrow$ 0;
(4) **for** each $p \in$ ND $-$ $\{k\}$ **do**
(5) **if** TV(k, p) > 0 **then**
(6) MT[p] $\Leftarrow$ TV(k, p), HP[p] $\Leftarrow$ 1;
(7) **else**
(8) MT[p] $\Leftarrow$ 0, HP[p] $\Leftarrow \infty$;
(9) **end if**
(10) **end for**
(11) Add k into VN;
(12) **while** ND $-$ VN $\neq \emptyset$ **do**
(13) Choose the node (named p) with the maximum local trust value from ND $-$ VN;
(14) **if** HP[p] < MH **then**
(15) **for** each $q \in$ ND $-$ VN $-$ $\{p\}$ **do**
(16) **if** TV(p, q) > 0 and MT[p] $*$ TV(p, q) $*$ (HP[p]/(HP[p] + 1))$^{\theta}$ > MT[q] **then**
(17) MT[q] $\Leftarrow$ MT[p] $*$ TV(p, q) $*$ (HP[p]/(HP[p] + 1))$^{\theta}$, HP[q] $\Leftarrow$ HP[p] + 1;
(18) **end if**
(19) **end for**
(20) **end if**
(21) Add p into VN;
(22) **end while**
(23) **return** MT;

Algorithm 1: Our MLT algorithm.

6. Aggregation Trust Evaluation

As we mentioned earlier, trust certificate-based and recommendation-based trust evaluations have diverse advantages and weaknesses as follows:

(a) Comparing to recommendation-based trust evaluation, trust certificate-based one can be conducted in a more fast and lightweight manner (the detailed analysis is provided in our previous work [12]) while it is intuitively more vulnerable to the collusion attack as the certifiers are strange to the trustor in most cases.

(b) Recommendation-based trust evaluation seems to be more credible than trust certificate-based one, as in the former only the ratings of trustworthy recommenders are considered. But collecting the opinions from trustworthy recommenders consumes large amounts of time and bandwidth resources, especially when MH is set as a relatively high value (e.g., 6).

Thus it is beneficial to aggregate these two kinds of trust evaluations to achieve the more accurate evaluation result. In our scheme, the final trust value FT(j, k) of trustee j in the sight of trustor k is calculated as

$$\mathrm{FT}(j,k) = \tau * \mathrm{CT}(j,k) + (1-\tau) * \mathrm{RT}(j,k), \quad (14)$$

where τ is a weight parameter within the range of $[0, 1]$ which controls the weights of two kinds of trust evaluations in aggregation trust evaluation. So the range of FT(j, k) is also 0~1. Specifically, when τ equals 1 or 0, the aggregation trust evaluation reduces to mere trust certificate-based one or mere recommendation-based one, respectively. In other cases (i.e., $0 < \tau < 1$), the aggregation trust evaluation falls in between trust certificate-based one and recommendation-based one.

7. Simulations and Analysis

To demonstrate the performance of our LSOT model, we present a series of simulations and analysis in this section. Specifically, we first deploy a fully distributed VANET scenario based on the famous Advogato dataset. Then we validate the variations of both average trust values and average acceptance rates of three kinds of messages. Moreover, we compare the evaluation performance of our proposed model with that of EBT and LCT models. Finally, we analyze and verify the robustness of our LSOT model against the collusion attack comparing to that of LCT model.

7.1. Simulation Settings. In this work, the comprehensive simulations are implemented by Java language on an Ubuntu server with 2.83 GHz CPU and 4 G RAM. In concrete terms, we first deploy a fully distributed VANET scenario: The trust recommendation network is built based on the famous Advogato dataset which includes 6541 nodes and 51127 directed edges (denoting three kinds of trust relationships among nodes, namely, apprentice, journeyer, and master, of

Table 2: Parameter settings in our simulations.

Parameters	Descriptions	Values
η	Number threshold in (3)	20
ω	Time window in (4)	100
α	Time decay factor in (4)	40
β	Constant in (5)	0.5
δ[1]	Distance threshold in (6)	∞
λ[1]	Distance decay factor in (6)	∞
μ	Default trust value in (8)	0.1
ϕ	Increment factor in (10)	0.2
ψ	Decrement factor in (11)	0.3
MH[2]	Maximum allowable hop in Algorithm 1	3
θ	Trust decay factor in (12)	0.5
ν	Default trust value in (13)	0.1
τ	Weight parameter in (14)	0.5

[1]As the nodes in Advogato dataset do not contain location information, we set $\delta = \infty$ and $\lambda = \infty$ in our simulations so as to ensure $\mathrm{WL}(i, k) \equiv 1$.
[2]MH is set as a relatively low value (i.e., 3) due to the highly dynamic and time-critical features of VANETs.

which corresponding trust values are 0.6, 0.8, and 1.0, resp.). The nodes' trust thresholds are randomly generated. Three kinds of different messages, namely, honest (i.e., authentic and helpful), general (i.e., authentic but valueless), and malicious (i.e., unreal and harmful) messages, are sent from different senders. In each test, a random node receives a message from certain sender and evaluates its trust value by utilizing our LSOT scheme. If the message's derived trust value reaches the node's trust threshold, the node accepts this message and provides a new trust certificate to the sender according to its satisfaction degree to this message. After each test, the timestamp adds 1. The parameters in our simulations are set as illustrated in Table 2.

7.2. Validating the Evaluation Performance. In this part, we mainly validate the average trust value variations of three kinds of messages in honest environment, and we also reveal the variations of average acceptation rates of three kinds of messages. In concrete terms, we divide the 500 times' tests into 5 equal intervals (i.e., I1~I5) and then calculate the average acceptation rate in each interval, respectively. The simulation is repeated 1000 times for each kind of messages and average results are shown in Figures 6 and 7.

We first analyze the variations of average trust values as shown in Figure 6. In the initial stage, three kinds of messages have the same trust value (i.e., 0.10). With the increase of test times (0~300 times), the average trust value of honest messages rises rapidly from 0.10 to 0.64 due to their excellent quality while that of general messages grows slowly from 0.10 to 0.36. Besides, the average trust value of malicious messages remains about the same at 0.10 on account of their terrible performance. In the latter tests (300~500 times), all the three kinds of messages dynamically keep constant average trust values (i.e., 0.64, 0.36, and 0.10, resp.).

Next, we analyze the variations of average acceptation rates as shown in Figure 7. In the first three intervals (i.e., I1~I3), the average acceptation rate of honest messages grows from 27.46% to 63.01% and that of general messages rises from

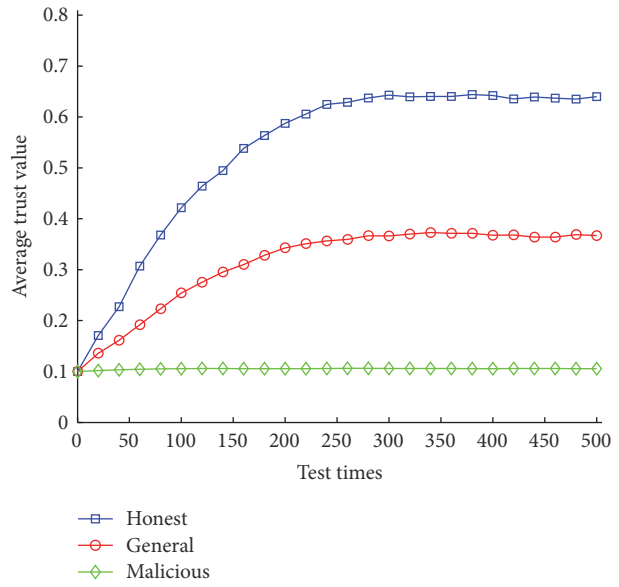


Figure 6: Average trust value variations of three kinds of messages in our LSOT model.

18.60% to 36.49%, while that of malicious messages basically stays unchanged at 11.43%. In the latter intervals (i.e., I4 and I5), all the three kinds of messages almost maintain constant average acceptation rates (i.e., 64.65%, 37.40%, and 11.43%, resp.).

As we know, honest messages bring benefits and malicious messages mean risks; thus the higher the average trust value and average acceptance rate of honest messages, the better, and the lower the average trust value and average acceptance rate of malicious messages, the better. Therefore, the above results show that our LSOT model significantly improves the average trust value and average acceptance rate of honest messages without increasing the risks caused by malicious messages.

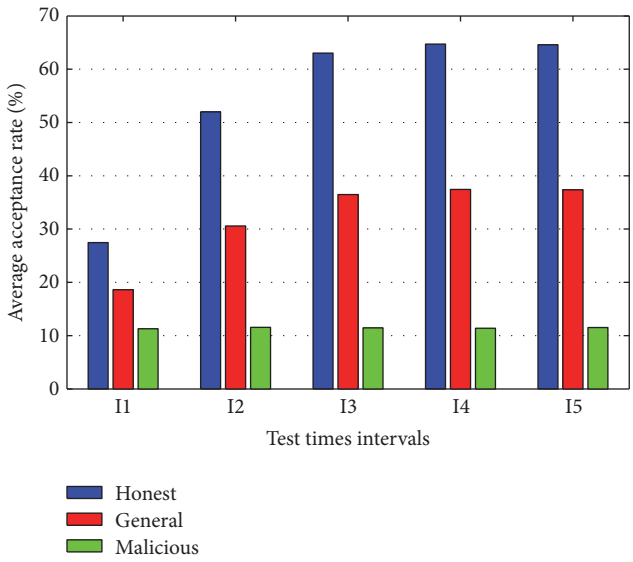


Figure 7: Average acceptation rate variations of three kinds of messages in our LSOT model.

7.3. Comparing the Evaluation Performance. In this simulation, we mainly compare the evaluation performance of our LSOT model with that of EBT and LCT models as they are similar to our model. Moreover, we deploy and necessarily modify these two models in our VANET scenario. As we know, the trust ranges in EBT and LCT models are $[-1, 1]$ and $[0, 100]$, respectively, different from that in our proposed model (i.e., $[0, 1]$); thus they are all converted to $[0, 1]$ for comparison. Besides, the role-based trust is removed from EBT model as it is not consistent with the fully self-organized way. This simulation is also repeated 1000 times for each kind of messages in EBT and LCT models, and the average results are shown in Figure 8. Moreover, we also compare the average acceptation rates of honest and general messages in every interval (i.e., I1~I5) in three kinds of models as illustrated in Figure 9.

We first analyze the average acceptation rate variations of honest messages in three kinds of trust models as demonstrated in Figure 9(a). In the first interval (i.e., I1), LCT model has distinctly lower average acceptation rate (i.e., 10.99%) than EBT model (i.e., 30.74%) and our LSOT model (i.e., 27.46%). It is because that LCT model merely includes trust certificate-based evaluation and the senders of honest messages are not able to provide sufficient trust certificates to improve their own trust values, while EBT model has no restriction about the number of recommenders in recommendation-based trust evaluation and the average trust value of honest messages rises with the increasing test times. Our LSOT model absorbs the merits of recommendation-based evaluation; thus in I1 the average acceptation rate in our LSOT model is greatly higher than that in LCT model and slightly lower than that in EBT model.

In the latter intervals (i.e., I2~I5), the average acceptation rate in EBT model rises slowly and then dynamically remains at a distinctly lower rate (i.e., 37.62%) than that in LCT model (i.e., 63.51%) and that in LSOT model (i.e., 64.10%). It is because EBT model only contains recommendation-based evaluation and a portion of recommenders cannot be reached within the maximum allowable hop (i.e., 3), while in LCT model the trust certificates are attached to the messages and they contribute to improving the trust values of honest messages. Our LSOT model includes the trust certificate-based and recommendation-based trust evaluations; thus in I2~I5 the average acceptation rate in our LSOT model is greatly higher than that in EBT model and generally higher than that in LCT model.

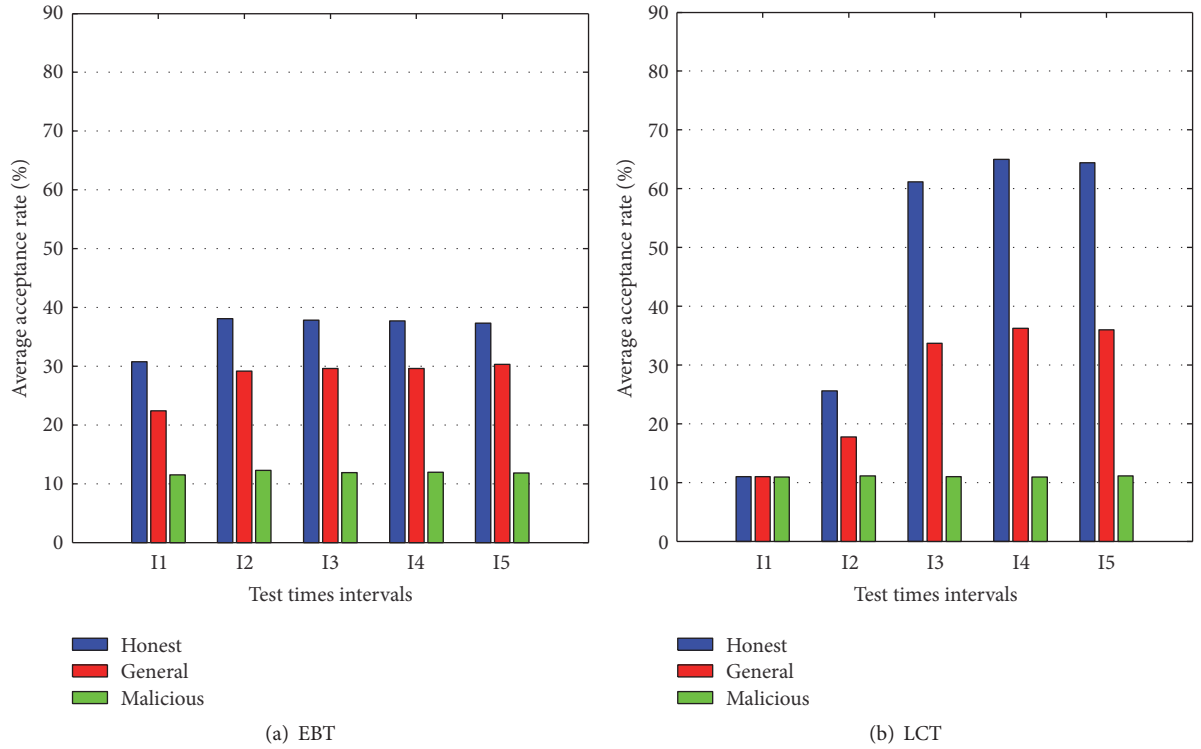
Next we analyze the average acceptation rate variations of general messages in three kinds of trust models as shown in Figure 9(b). In the first interval (i.e., I1), the average acceptation rate in our LSOT model (i.e., 18.60%) is greatly higher than that in LCT model (i.e., 10.98%) and slightly lower than that in EBT model (i.e., 22.41%). In the latter intervals (i.e., I2~I5), the average acceptation rate in our LSOT model rises rapidly and stays basically unchanged at a relatively higher rate (i.e., 37.09%) than that in EBT model (i.e., 29.84%) and LCT model (i.e., 35.30%). The detailed analysis is omitted as it is similar to that of honest messages.

Besides, we analyze the average acceptation rate variations of malicious messages in three kinds of trust models (as the average acceptation rate of malicious messages in every model remains about the same as 11.46%, the comparison chart is omitted for space limitation). In LCT model, the senders of malicious messages act as newcomers and refuse to provide any unfavorable trust certificates; thus both the average trust value and average acceptation rate keep largely constant. In EBT model, due to the malicious behaviors and "reentry" strategy [41], the average trust value and average acceptation rate of malicious messages also remain basically unchanged. Our LSOT model aggregates EBT and LCT models; thus the average acceptation rate of malicious messages also remains largely untouched.

Through the above analysis, we can easily discover that our LSOT model not only limits the risks caused by malicious messages as well as EBT and LCT models do but also greatly raises the average acceptation rate of honest messages and improves that of general messages to some extent when comparing to the other trust models. Thus our LSOT model has better evaluation performance than EBT and LCT models in general.

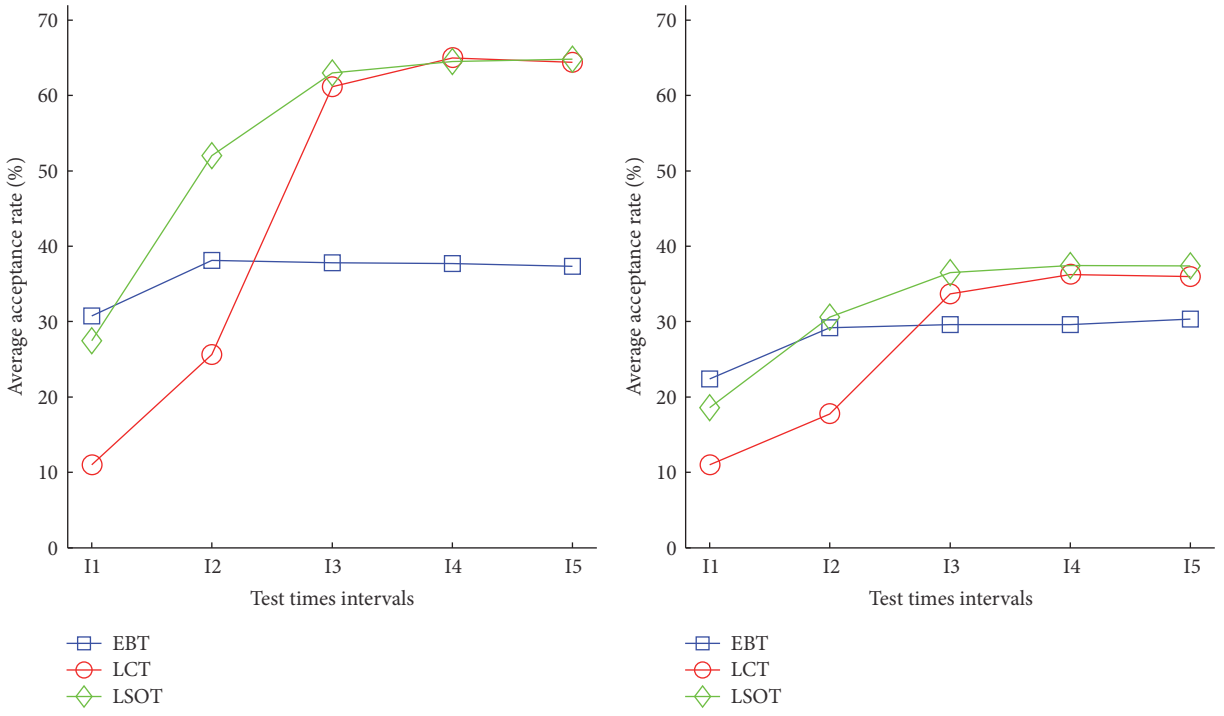
7.4. Comparing the Robustness Characteristics. In the previous parts, we mainly consider the performance of our model in honest environment, while in this part we focus on verifying and analyzing the robustness of our model against the collusion attack through comparing to that of LCT model. The comparison with EBT model is omitted as there is no consideration of collusion attack in this model. Due to the distributed feature of VANETs, malicious nodes may collude with other nodes to raise their own trust values (i.e., ballot stuffing) or slander their honest competitors (i.e., bad mouthing) [42], which will bring risks to message receivers. So a good trust model for VANETs should be able to detect and filter them out.

As we well know, in the trust certificate-based trust evaluation the certifiers are strange to the active trustor, while



(a) EBT (b) LCT

Figure 8: Average acceptation rate variations of three kinds of messages in EBT and LCT models.



(a) Honest (b) General

Figure 9: Average acceptation rate comparisons of honest and general messages in three kinds of trust models.

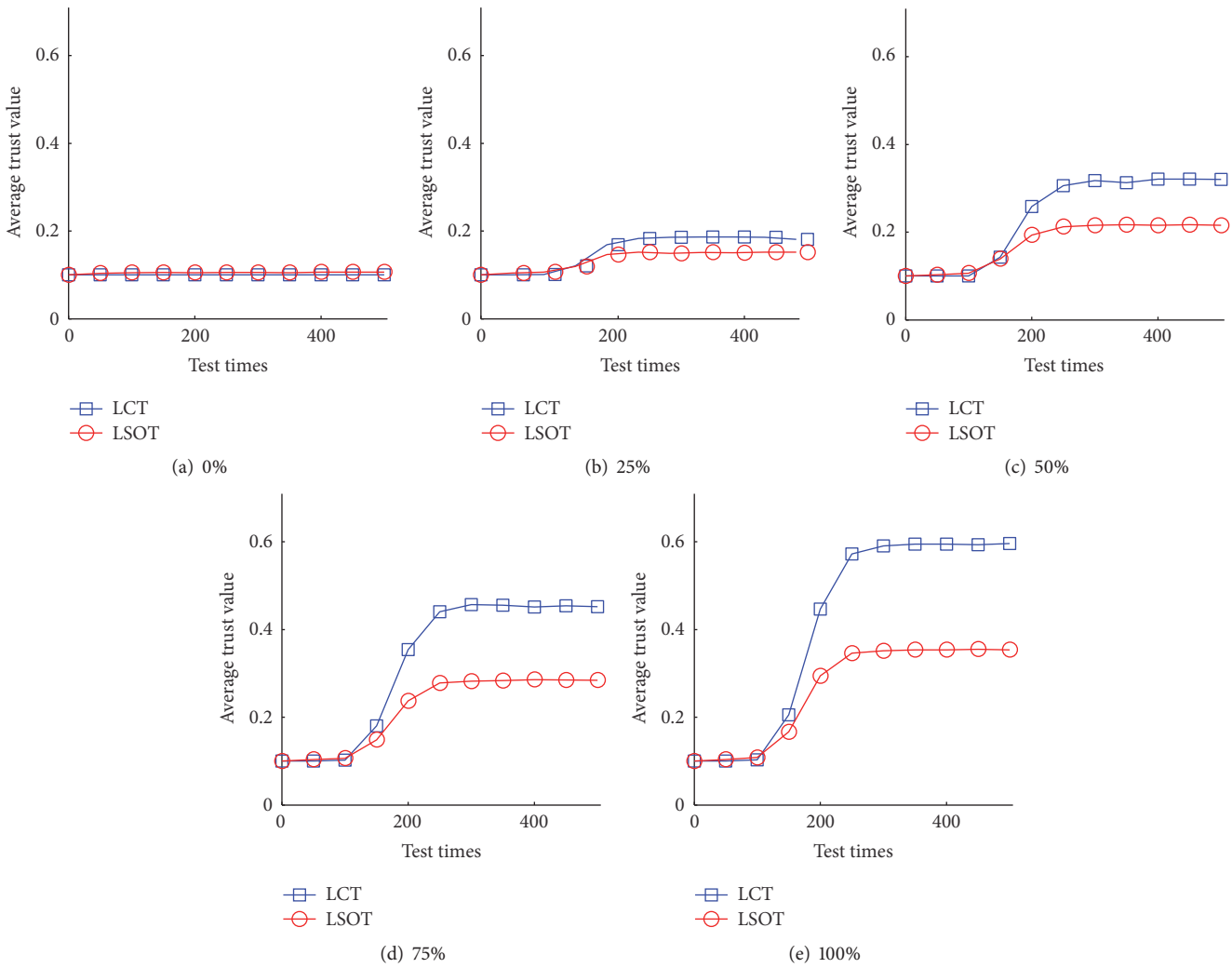


Figure 10: Average acceptation rate comparisons of malicious messages with different PCC values.

in the recommendation-based trust evaluation the recommenders are trustworthy in the perspective of active trustor. Thus the certifiers have a higher likelihood of colluding with malicious senders than the recommenders. LCT model merely consists of the trust certificate-based trust evaluation; thus it is intuitively vulnerable to the collusion attack. While our LSOT model aggregates the trust certificate-based and recommendation-based trust evaluations, it has relatively strong robustness against the collusion attack.

Next, we validate the above analysis through two simulations in which the recommenders are assumed to be trustworthy and the certifiers may be collusive at a certain percentage (e.g., 0%, 25%, 50%, 75%, or 100%).

7.4.1. Ballot Stuffing. In this part, we compare the robustness against the ballot stuffing of our LSOT model with that of LCT model. In the ballot stuffing, the collusive certifiers provide favorable trust certificates with high rating values to malicious messages in spite of their bad performance. In each simulation, we vary the Percentage of Collusive Certifiers (PCC) and then calculate the average trust value of malicious messages in each case, respectively. The simulation is repeated 1000 times and the average results are illustrated in Figure 10.

In the ideal case (i.e., PCC = 0%) as shown in Figure 10(a), the variation curves of average trust values of malicious messages in two kinds of trust models are very close to each other. With the increase of PCC, the curve in LCT model gets steeper and steeper while that in our LSOT model rises slowly, so the gap of two curves gradually grows. In the extreme case (i.e., PCC = 100%) as shown in Figure 10(e), the gap of two curves reaches the maximum amount and the average trust value of malicious message in our LSOT model is significantly lower than that in LCT model.

As we mentioned earlier, the lower the average trust value of malicious messages, the better; thus the above simulation and analysis results demonstrate that our LSOT model has stronger robustness against the ballot stuffing than LCT model.

7.4.2. Bad Mouthing. In this part, we validate the robustness of our LSOT model against the bad mouthing through comparing to LCT model. In the bad mouthing, the collusive

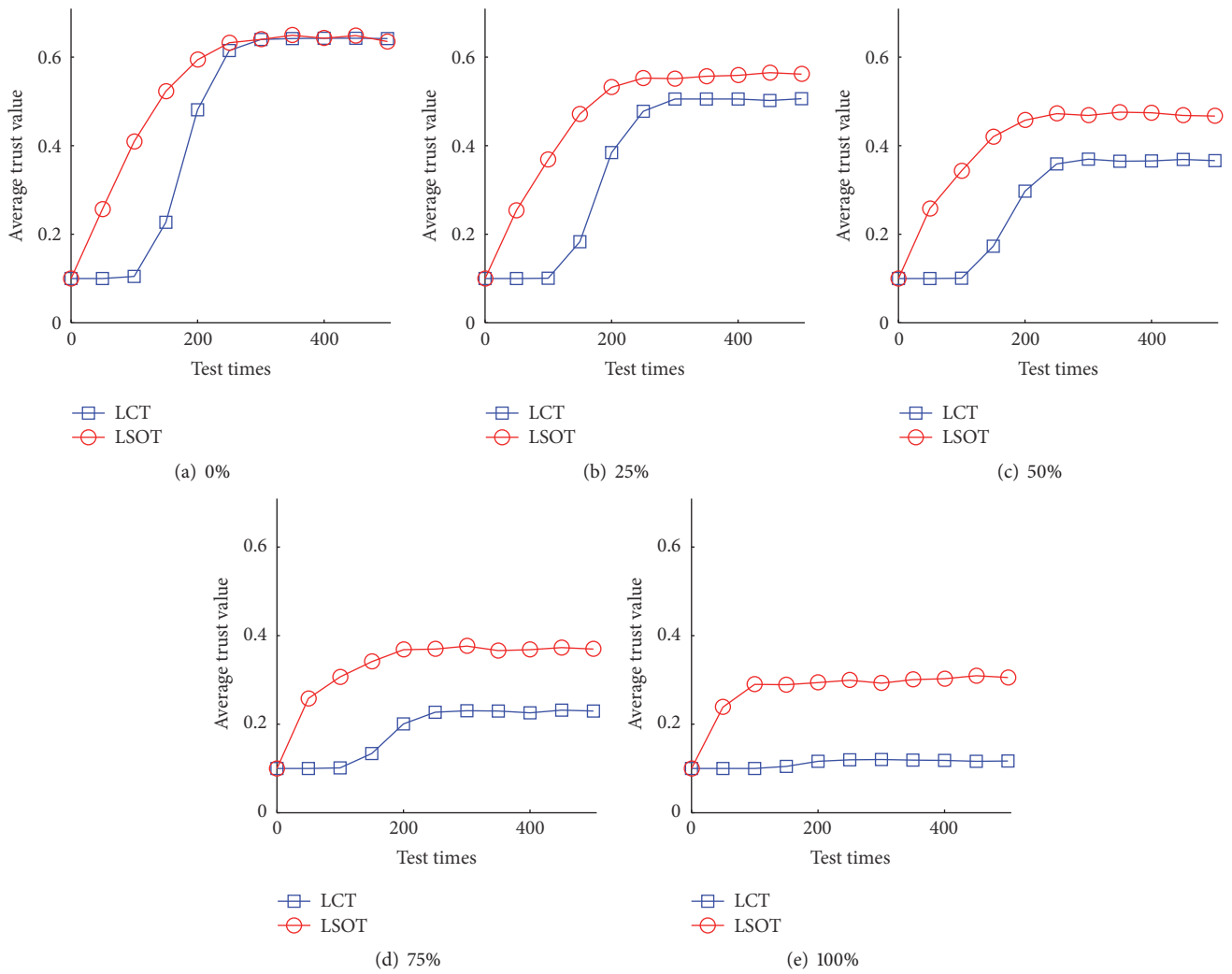


Figure 11: Average acceptation rate comparisons of honest messages with different PCC values.

certifiers provide adverse trust certificates with low rating values to honest messages in spite of their good quality. In each simulation, we vary PCC and compute the average trust value of honest messages in each case, respectively. The simulation is also repeated 1000 times and average outputs are demonstrated in Figure 11.

In the ideal case (i.e., PCC = 0%) as shown in Figure 11(a), the variation curve of average trust value of honest messages in our LSOT model is approximately consistent with that in LCT model. With the increase of PCC, the curve growth in LCT model becomes slower and slower while that in our LSOT model is relatively fast; thus the gap of two variation curves progressively grows. In the extreme case (i.e., PCC = 100%) as shown in Figure 11(e), the gap of two curves is up to the maximum value and the average trust value of honest messages in our LSOT model is greatly higher than that in LCT model.

As mentioned earlier, the higher the average trust value of honest messages, the better; thus the above simulation and analysis results illustrate that our LSOT model significantly outperforms LCT model in terms of the robustness against the bad mouthing.

8. Conclusion

In this work, we have proposed a novel LSOT model, in which both the supernodes and trusted third parties are not needed, for VANETs in a self-organized way. It combines both trust certificate-based and recommendation-based trust evaluations; thus the evaluation in it can be made quickly and reaches an excellent performance in a lightweight manner. In trust certificate-based trust evaluation, we have comprehensively considered three factor weights, namely, number weight, time decay weight, and context weight, to ease the collusion attack and make the evaluation result more accurate. In recommendation-based trust evaluation, we have utilized the testing interaction method to build and maintain the trust network and proposed an effective MLT algorithm to identify trustworthy recommenders. Moreover, we have deployed a fully distributed VANET scenario based on the celebrated

Advogato dataset and conducted comprehensive simulations and analysis. The results illustrate that our LSOT model greatly overmatches the outstanding EBT and LCT models in terms of both evaluation performance and robustness against the collusion attack.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported by National High Technology Research and Development Program (863 Program) (no. 2015AA016007), Key Program of NSFC Grant (no. U1405255), Major Natural Science Foundation of China (no. 61370078), National Natural Science Foundation of China (no. 61502375, no. 61303218), Natural Science Basis Research Plan in Shaanxi Province of China (no. 2016JQ6046), and Science and Technology Project of Shaanxi Province (no. 2016JM6007).

References

[1] J. Zhang, "Trust management for VANETs: challenges, desired properties and future directions," *International Journal of Distributed Systems and Technologies*, vol. 3, no. 1, pp. 48–62, 2012.

[2] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: an effective strategy for location privacy in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 86–96, 2012.

[3] H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 6, pp. 164–171, 2008.

[4] D. Zelikman and M. Segal, "Reducing interferences in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 3, pp. 1582–1587, 2015.

[5] S. S. Tangade and S. S. Manvi, "A survey on attacks, security and trust management solutions in VANETs," in *Proceedings of the 4th International Conference on Computing, Communications and Networking Technologies (ICCCNT '13)*, pp. 1–6, IEEE, Tiruchengode, India, July 2013.

[6] S. Gillani, F. Shahzad, A. Qayyum, and R. Mehmood, "A survey on security in vehicular ad hoc networks," in *Communication Technologies for Vehicles*, pp. 59–74, Springer, Berlin, Germany, 2013.

[7] J. Grover, M. S. Gaur, and V. Laxmi, "Trust establishment techniques in VANET," in *Wireless Networks and Security*, Signals and Communication Technology, pp. 273–301, Springer, Berlin, Germany, 2013.

[8] S. Park, B. Aslam, and C. C. Zou, "Long-term reputation system for vehicular networking based on vehicle's daily commute routine," in *Proceedings of the 2011 IEEE Consumer Communications and Networking Conference (CCNC '11)*, pp. 436–441, Las Vegas, Nev, USA, January 2011.

[9] X. Li, J. Liu, X. Li, and W. Sun, "RGTE: a reputation-based global trust establishment in VANETs," in *Proceedings of the 5th IEEE International Conference on Intelligent Networking and Collaborative Systems (INCoS '13)*, pp. 210–214, IEEE, Xi'an, China, September 2013.

[10] T. D. Huynh, N. R. Jennings, and N. R. Shadbolt, "Certified reputation: how an agent can trust a stranger," in *Proceedings of the 5th ACM International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS '06)*, pp. 1217–1224, ACM, May 2006.

[11] Z. Huang, S. Ruj, M. A. Cavenaghi, M. Stojmenovic, and A. Nayak, "A social network approach to trust management in VANETs," *Peer-to-Peer Networking and Applications*, vol. 7, no. 3, pp. 229–242, 2014.

[12] Z. Liu, J. Ma, Z. Jiang, and Y. Miao, "LCT: a lightweight cross-domain trust model for the mobile distributed environment," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 2, pp. 914–934, 2016.

[13] F. Qu, Z. Wu, F. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.

[14] J. Zhang, "A survey on trust management for VANETs," in *Proceedings of the 25th IEEE International Conference on Advanced Information Networking and Applications (AINA '11)*, pp. 105–112, Singapore, March 2011.

[15] J. Jakubiak and Y. Koucheryavy, "State of the art and research challenges for VANETs," in *Proceedings of the 5th IEEE Consumer Communications and Networking Conference (CCNC '08)*, pp. 912–916, IEEE, Las Vegas, Nev, USA, January 2008.

[16] D. Wang, T. Muller, Y. Liu, and J. Zhang, "Towards robust and effective trust management for security: a survey," in *Proceedings of the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom '14)*, pp. 511–518, IEEE, Beijing, China, September 2014.

[17] N. J. Patel and R. H. Jhaveri, "Trust based approaches for secure routing in VANET: a survey," *Procedia Computer Science*, vol. 45, pp. 592–601, 2015.

[18] A. Wu, J. Ma, and S. Zhang, "RATE: a RSU-aided scheme for data-centric trust establishment in VANETs," in *Proceedings of the 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '11)*, pp. 1–6, IEEE, Wuhan, China, September 2011.

[19] F. Gómez Mármol and G. Martínez Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 934–941, 2012.

[20] N. Yang, "A similarity based trust and reputation management framework for VANETs," *International Journal of Future Generation Communication and Networking*, vol. 6, no. 2, pp. 25–34, 2013.

[21] W. Bamberger, J. Schlittenlacher, and K. Diepold, "A trust model for intervehicular communication based on belief theory," in *Proceedings of the 2nd IEEE International Conference on Social Computing (SocialCom '10)*, pp. 73–80, IEEE, Minneapolis, Minn, USA, August 2010.

[22] X. Hong, D. Huang, M. Gerla, and Z. Cao, "SAT: situation-aware trust architecture for vehicular networks," in *Proceedings of the 3rd International Workshop on Mobility in the Evolving Internet Architecture, MobiArch'08*, pp. 31–36, USA, August 2008.

[23] Z. Huang, S. Ruj, M. Cavenaghi, and A. Nayak, "Limitations of trust management schemes in VANET and countermeasures," in *Proceedings of the IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '11)*, pp. 1228–1232, IEEE, Toronto, Canada, September 2011.

[24] P. Wex, J. Breuer, A. Held, T. Leinmüller, and L. Delgrossi, "Trust issues for vehicular ad hoc networks," in *Proceedings of the IEEE 67th Vehicular Technology Conference (VTC '08)*, pp. 2800–2804, Singapore, May 2008.

[25] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile Ad Hoc vehicular networks," *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, vol. 41, no. 3, pp. 407–420, 2011.

[26] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, "A trust modeling framework for message propagation and evaluation in VANETs," in *Proceedings of the 2nd International Conference on Information Technology Convergence and Services (ITCS '10)*, pp. 1–8, August 2010.

[27] M. Saini, A. Alelaiwi, and A. El Saddik, "How close are we to realizing a pragmatic VANET solution? A meta-survey," *ACM Computing Surveys*, vol. 48, no. 2, article 29, 2015.

[28] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: a survey on architecture, challenges, and solutions," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2377–2396, 2015.

[29] T. Ma, J. Zhou, M. Tang et al., "Social network and tag sources based augmenting collaborative recommender system," *IEICE Transactions on Information and Systems*, vol. E98.D, no. 4, pp. 902–910, 2015.

[30] H. Li, D. Liu, Y. Dai, and T. H. Luan, "Engineering searchable encryption of mobile cloud networks: when QoE meets QoP," *IEEE Wireless Communications*, vol. 22, no. 4, pp. 74–80, 2015.

[31] A. M. Shabut, K. P. Dahal, S. K. Bista, and I. U. Awan, "Recommendation based trust model with an effective defence scheme for MANETs," *IEEE Transactions on Mobile Computing*, vol. 14, no. 10, pp. 2101–2115, 2015.

[32] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1228–1237, 2015.

[33] J. Shen, H. W. Tan, J. Wang, J. W. Wang, and S. Y. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," *Journal of Internet Technology*, vol. 16, no. 1, pp. 171–178, 2015.

[34] S. Xie and Y. Wang, "Construction of tree network with limited delivery latency in homogeneous wireless sensor networks," *Wireless Personal Communications*, vol. 78, no. 1, pp. 231–246, 2014.

[35] B. Qureshi, G. Min, and D. Kouvatsos, "A distributed reputation and trust management scheme for mobile peer-to-peer networks," *Computer Communications*, vol. 35, no. 5, pp. 608–618, 2012.

[36] T. D. Huynh, N. R. Jennings, and N. R. Shadbolt, "An integrated trust and reputation model for open multi-agent systems," *Autonomous Agents and Multi-Agent Systems*, vol. 13, no. 2, pp. 119–154, 2006.

[37] T. Tran and R. Cohen, "A reliability modelling based strategy to avoid infinite harm from dishonest sellers in electronic marketplaces," *Journal of Business and Technology, Special Issue on Business Agents and the Semantic Web*, vol. 1, no. 1, pp. 69–76, 2005.

[38] Z. Liu, J. Ma, Z. Jiang, Y. Miao, and C. Gao, "IRLT: integrating reputation and local trust for trustworthy service recommendation in service-oriented social networks," *PLoS ONE*, vol. 11, no. 3, Article ID e0151438, 2016.

[39] G. Liu, Y. Wang, and M. A. Orgun, "Trust transitivity in complex social networks," in *Proceedings of the 25th AAAI Conference on Artificial Intelligence (AAAI '11)*, vol. 11, pp. 1222–1229, San Francisco, Calif, USA, August 2011.

[40] Y. A. Kim and H. S. Song, "Strategies for predicting local trust based on trust propagation in social networks," *Knowledge-Based Systems*, vol. 24, no. 8, pp. 1360–1371, 2011.

[41] A. Jøsang and J. Golbeck, "Challenges for robust trust and reputation systems," in *Proceedings of the 5th International Workshop on Security and Trust Management (SMT '09)*, Saint Malo, France, September 2009.

[42] S. Liu, H. Yu, C. Miao, and A. C. Kot, "A fuzzy logic based reputation model against unfair ratings," in *Proceedings of the 12th International Conference on Autonomous Agents and Multi-Agent Systems (AAMAS '13)*, pp. 821–828, St. Paul, Minn, USA, May 2013.