TCEMD: A Trust Cascading-Based Emergency Message Dissemination Model in VANETs

Zhiquan Liu, Jian Weng, Jianfeng Ma, Jingjing Guo, Bingwen Feng, Zhongyuan Jiang, and Kaimin Wei

***Abstract*—Vehicular ad-hoc networks (VANETs) have recently attracted considerable attention from both industry and academia for improving road safety and traffic efficiency. Trust modeling plays a significant role in VANETs, however, the existing trust models cannot primely conform to the characteristics of VANETs. This article proposes a novel trust cascading-based emergency message dissemination (TCEMD) model which incorporates the entity-oriented trust values into data-oriented trust evaluation in an efficient manner. In the proposed model, when an emergency event (e.g., an obstacle in front of the road) occurs, the emergency messages can be disseminated among the nearby vehicles in a trust cascading manner, where the entity-oriented trust values (which are evaluated and updated by leveraging the trust certificates and are contained in the messages) are adopted as important weights. Subsequently, the theoretical analysis for the robustness against several kinds of attacks and malicious behaviors, failure tolerance features, compatibility for several kinds of special situations, and incentive mechanisms in the TCEMD model are detailed. Afterwards, a series of simulations and analyses are conducted in a typical highway environment, and the results reveal that the proposed model significantly outperforms the existing models in several cases.**

***Index Terms*—Data-oriented trust, emergency message dissemination, entity-oriented trust, trust cascading, trust model, vehicular ad-hoc networks (VANETs).**

Manuscript received August 13, 2019; revised November 1, 2019; accepted November 27, 2019. Date of publication December 4, 2019; date of current version May 12, 2020. This work was supported in part by the National Natural Science Foundation of China under Grant 61802146, Grant U1736203, Grant 61602360, Grant 61825203, Grant 61932011, Grant 61972178, Grant 61802145, Grant 61906075, and Grant 61932010, in part by the Guangdong Basic and Applied Basic Research Foundation under Grant 2019A1515011017, in part by the Natural Science Foundation of Guangdong Province under Grant 2018A030313813, Grant 2017A030313334, Grant 2019B010136003, Grant 2019B010137005, Grant 2017A030313390, and Grant 2018A030313387, in part by the Science and Technology Program of Guangzhou of China under Grant 201802010061 and Grant 201804010428, in part by the Fundamental Research Funds for the Central Universities under Grant 11618332, Grant 11617343, Grant JBX181504, and Grant BDZ011402, in part by the Guangdong Key Laboratory of Data Security and Privacy Preserving under Grant 2017B03031004, and in part by the Scientific and Technological Project under Grant 2019AB001. *(Corresponding author: Bingwen Feng.)*

Z. Liu, J. Weng, B. Feng, and K. Wei are with the College of Cyber Security, Jinan University, Guangzhou 510632, China, and also with the Guangdong Key Laboratory of Data Security and Privacy Preserving, Jinan University, Guangzhou 510632, China (e-mail: zqliu@jnu.edu.cn; cryptjweng@gmail.com; bingwfeng@gmail.com; weikaimin@gmail.com).

J. Ma, J. Guo, and Z. Jiang are with the School of Cyber Engineering, Xidian University, Xi'an 710071, China (e-mail: jfma@mail.xidian.edu.cn; jjguo@xidian.edu.cn; zyjiang@xidian.edu.cn).

Digital Object Identifier 10.1109/JIOT.2019.2957520

I. Introduction

NOWADAYS, with the progress of wireless communication, position, and embedded technologies, vehicular ad-hoc networks (VANETs) have become one of the most prominent branches of mobile ad-hoc networks (MANETs) and a primary component of intelligent transportation system (ITS) due to their tremendous potential to improve road safety and traffic efficiency [1]–[3]. The primary idea of VANETs is that vehicles and roadside units (RSUs) adopt the advanced wireless communication technologies to achieve both vehicle-to-vehicle (V2V) and vehicle-to-RSU (V2R) communications in a single-hop or multihop way and form a highly dynamic ad-hoc network [4], [5], as shown in Fig. 1.

In recent years, VANETs have attracted considerable attention from both industry and academia, where the cooperative safety applications are one of the most significant branches [6]. Through the emergency message dissemination in the V2V and V2R manners, the cooperative safety applications enable each vehicle to intelligently perceive the conditions of surrounding vehicles and roads and make decisions about potential dangers in advance, so as to observably reduce the urgency degree that each vehicle copes with emergency events and then improve road safety and traffic efficiency [7].

So far, a large number of schemes have been put forward for emergency message dissemination in VANETs from the perspective of improving communication reliability and reducing message dissemination latency [4], [8]–[13]. These schemes can be roughly classified into four categories, namely, distance-based, location-based, cluster-based, and probabilistic-based schemes [14]. They provide a great many brilliant ideas, but unfortunately there is no special consideration about potential attacks and malicious behaviors in their schemes.

In practice, VANETs are vulnerable to attacks and malicious behaviors (e.g., unreal information, impersonation, suspension, eavesdropping, hardware tampering, etc. [15]) due to the large, open, sparse, and highly dynamic characteristics [7]. To resist against attacks and malicious behaviors, quite a lot of studies have been conducted by leveraging digital signature and cryptography technologies [3], [16]–[21]. These studies generally focus on ensuring vehicles' authenticity and privacy as well as messages' confidentiality and integrality, rather than evaluating vehicles' trustworthiness and messages' quality [22].

In fact, however, due to the complex road environment and limited perception and processing ability, an authenticated and honest vehicle may broadcast unreal emergency messages with a certain probability. Furthermore, an

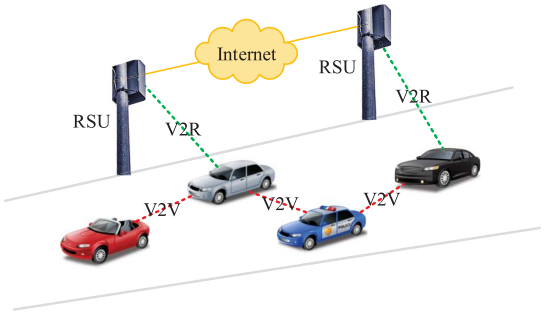


Fig. 1. Schematic of VANETs.

authenticated but malicious vehicle may try its utmost to broadcast unreal emergency messages for deceiving others. Moreover, in the classic authorization and revocation schemes based on digital signature and cryptography technologies, message receivers cannot perceive message broadcasters' trustworthiness and received messages' quality in advance, so these schemes cannot primely fulfill the requirements of VANETs [23].

Trust modeling plays a crucial role in VANETs as it enables each vehicle to evaluate other vehicles' trustworthiness as well as received messages' quality in advance, aiming at avoiding the dire consequences caused by unreal emergency messages [24]. At present, trust modeling in VANETs is at a relatively early stage, and based on architecture, the existing trust models can be roughly divided into two classes, namely, infrastructure-based and self-organized models [25].

Infrastructure-based trust models usually contain a centralized authority (CA) which is tasked with maintaining the trust value of each vehicle/event, and each vehicle requests CA for the latest trust value of target vehicle/event. Such trust models are generally easy to manage, control, and protect, and are in line with the practice that vehicles are usually managed by the traffic safety administration (TSA, which is a CA in essence) [26]. However, they generally incur relatively large time delay and bring some inconvenience. For example, CA is required to stay online all the time, and every vehicle is required to be able to connect to CA at any time any where [27]. In practice, however, CA may break down for a short period of time, and vehicles cannot access to CA at some places where RSUs are not available [28].

In self-organized trust models, CA is not required and every vehicle evaluates the trust value of target vehicle/event based on the local knowledge obtained from its own past experiences and other vehicle' recommendations in a short period of time. Such trust models generally can overcome the CA bottleneck and reduce the time delay in infrastructure-based trust models. However, due to the highly dynamic feature of VANETs, the oneself's past experiences are unavailable to trust evaluation in most cases [26]. Besides, collecting the trust recommendations from other vehicles usually causes a huge waste of bandwidth and time, which does not satisfy the requirements of VANETs well [29].

Meanwhile, according to evaluation object, the existing trust models can be broadly classified into two types, namely, entity-oriented and data-oriented models[1] [25].

In entity-oriented trust models, the trust relationships among vehicles are usually built based on similarity, experience, role, and so forth [32], [33], and if vehicle A trusts vehicle B, then vehicle A trusts all of the messages from vehicle B, and vice versa. In fact, however, as mentioned earlier, road environment and a vehicle's perception and processing ability have marked impacts on the quality of its messages, so a vehicle's trust level cannot fully reflect the quality of its messages [30], [34].

Data-oriented trust models generally focus on evaluating the trust of received message, instead of that of the vehicle which broadcasts the message [30]. Such models usually assume that every vehicle receives several messages about an emergency event from distinct neighboring vehicles and decides whether to trust the emergency event by leveraging the trust evaluation based on the Dempster–Shafer theory, Bayesian inference, social network theory, majority voting (MV), and so forth [30], [31], [35]. These models generally fully ignore entity-oriented trust and assign the same weight to the messages from honest and malicious vehicles, thus cannot perform well in practice [25].

In order to establish an efficient and robust trust model for emergency message dissemination in VANETs and overcome the aforementioned deficiencies in previous work, we propose a trust cascading-based emergency message dissemination (TCEMD) model in this article, and the main contributions of this article are summarized as follows.

1) This article not only details the proposal of trust cascading in VANETs but also puts forward a novel TCEMD model which is quite different from the existing models, for instance, linear threshold (LT) [36], MV [31], countering information oversampling (CIO) [35], and reputation-based announcement (RA) [26] models. The LT model merely considers the influence of a single factor while our model considers the influences of two opposite factors together; MV and CIO models completely ignore entity-oriented trust while our model incorporates entity-oriented trust values into data-oriented trust evaluation in an efficient manner; RA model considers each message about an emergency event in isolation while our model considers as many as possible messages reporting different statuses of an emergency event together. Consequently, our model primely overcomes the deficiencies of LT, MV, CIO, and RA models.
2) This article details the motivations and various stages in the TCEMD model. The motivations include: a) incorporating the entity-oriented trust values into data-oriented trust evaluation; b) considering the messages reporting different statuses of an emergency event together; c) considering as many as possible messages from distinct broadcasters together; and d) utilizing trust certificate to derive entity-oriented trust value. Besides, the various stages

[1] In some related work [23], [30], [31], entity is also named as node/vehicle, and data is also called as message/report. They alternately appear in this article.

include: a) the initialization of CA and RSUs; b) vehicle registration; c) trust certificate requesting; d) emergency message dissemination; e) trust feedback reporting; f) trust information updating; and g) vehicle revocation.

3) The TCEMD model is of high performance in several cases. To demonstrate the performance of the TCEMD model, we present the theoretical analysis for the robustness against several kinds of attacks and malicious behaviors, failure tolerance features, compatibility for several kinds of special situations, and incentive mechanisms in the TCEMD model in detail. Subsequently, we deploy a typical highway environment by leveraging the famous SUMO[2] simulator, and conduct comprehensive simulations and analysis. We verify the performance of the TCEMD model and compare it with MV, CIO, and RA models. The results demonstrate that the TCEMD model is significantly superior to the other models in several cases.

The remainder of this article is organized as follows. Section II introduces some related work and its limitations, and Section III details the motivations, proposal of trust cascading, primary elements, formalized notations and definitions. Then, Section IV describes the various stages in the TCEMD model, and Section V elaborates the theoretical analysis for the robustness, failure tolerance features, compatibility for several kinds of special situations, and incentive mechanisms. Subsequently, comprehensive simulations and analysis are presented in Section VI, followed by the conclusion and future work in Section VII.

II. Related Work

In the past years, as one of the most significant branches of VANETs, the cooperative safety applications have been widely studied in both industry and academia [6], and many schemes have been proposed for emergency message dissemination in VANETs with a view to improving communication reliability and reducing message dissemination latency [4], [8]–[13]. Chen *et al.* [14] classified them into probabilistic-based, distance-based, location-based, and cluster-based schemes, but unfortunately there is no special attention to potential attacks and malicious behaviors in these schemes [37].

To resist against attacks and malicious behaviors, plenty of researches have been conducted by leveraging digital signature and cryptography technologies [3], [16]–[21]. These researches mainly aim at ensuring vehicles' authenticity and privacy as well as messages' confidentiality and integrality. Lu *et al.* [3] came up with a dynamic privacy-preserving key management scheme (named as DIKE) for location-based services (LBSs) in VANETs. Their scheme can achieve vehicle users' privacy preservation while improving the key update efficiency. Jiang *et al.* [21] proposed a novel anonymous batch authentication scheme (called as ABAH) to replace the certificate revocation list checking process. Their scheme can reduce the verification delay than the conventional authentication methods employing certificate revocation lists and can also keep conditional privacy in VANETs. These schemes pay little attention to evaluating vehicles' trustworthiness and messages' quality [22]. However, as mentioned earlier, an authenticated vehicle is also likely to broadcast unreal messages for some reasons and other vehicles cannot perceive them in advance.

Trust modeling has been proved to be an effective solution for mobile distributed environments, and plays a crucial role in VANETs as it enables each vehicle to evaluate other vehicles' trustworthiness and received messages' quality in advance so as to avoid the dire consequences caused by unreal messages [24]. So far, a large number of trust models have been proposed for MANETs [38], wireless sensor networks (WSNs) [39], mobile peer-to-peer networks (MP2Ps) [40], mobile crowd-sensing (MCS) [41], and LBS recommendation (LBSR) [42], however, they cannot be applied well to VANETs due to the unique characteristics and requirements. At present, trust modeling in VANETs is still at its relatively early stage. According to architecture, the existing trust models in VANETs can be roughly separated into infrastructure-based and self-organized models, and according to evaluation object, they can be broadly categorized into entity-oriented and data-oriented models [25].

Infrastructure-Based: Li *et al.* [43] proposed a reputation-based global trust establishment (RGTE) model in which the reputation management center (RMC) is responsible for both collecting trust information from legal vehicles and calculating their reputation scores, and each vehicle needs to request RMC for the latest reputation list containing all the potential target vehicles frequently, which usually causes a waste of bandwidth and time. Meanwhile, in RGTE model, RMC must be available and accessible all the time to every vehicle. Li *et al.* [26] put forward a mere RA model, in which the centralized reputation server (RS) is responsible for maintaining the reputation scores of vehicles, and access points (APs) act as the communication interfaces between RS and vehicles. Their work aggregates asymmetric cryptography, digital signature, and reputation certificate so as to put forward a robust trust scheme for emergency message dissemination in VANETs. However, in RA model, a message's quality depends fully on its broadcaster's reputation score, which overlooks the fact that even quite an honest vehicle may also broadcast unreal messages with a certain probability due to the complex road environment and limited perception and processing ability. In addition, their study only considers the message broadcasting and trust evaluation among single-hop vehicles, which greatly limits its applicability.

Self-Organized: Bamberger *et al.* [44] noted that most of vehicles meet each other frequently in a small town, and put forward a novel belief theory-based trust (BTT) model which mainly focuses on the direct experiences of vehicles, instead of on a system-wide reputation that usually depends on a central unit. Their scheme integrates different components and models trust as a social mechanism to handle the uncertainty in inter-vehicular information exchange. However, their work depends on vehicles' direct experiences too much, therefore BTT model is not suitable to the general VANET environment, in which it is widely considered that the same two vehicles seldom meet each other more than once [33], [45], [46]. Wang *et al.* [47]

[2]Simulation of Urban Mobility: http://sumo.dlr.de.

presented a novel concept of attribute similarity, and proposed a simple attribute similarity-based trust propagation (ASTP) model, in which the similarity degree of attributes are calculated to discover potential friendly vehicles among strangers. Their work can improve the reliability of packet delivery over multihop routes to some degree in the presence of potential package dropping probability. Nevertheless, in ASTP model, malicious vehicles can modify their attributes on purpose to deceive other vehicles. Furthermore, only taking the attribute similarity into consideration is far from adequate for selecting reliable routes.

Entity-Oriented: Gazdar *et al.* [48] proposed a distributed advanced analytical trust (DAAT) model based on a Markov chain for formalizing the trust metric variation and its stability in VANETs. The DAAT model considers not only the dynamic trust metric variation according to the vehicle behaviors but also the constraints related to the monitoring process, and can filter out malicious and selfish vehicles effectively. However, this model merely aims at establishing trust relationships among vehicles, and does not take evaluating data's quality into consideration. In our previous work [23], we put forward a novel lightweight self-organized trust (LSOT) model which includes both trust certificate-based and recommendation-based evaluation modules. Both supernodes and trusted third parties are not required in this model. Nevertheless, the LSOT model does not distinguish between the trust value of a message and that of its broadcaster. That is, the trust value of a message is completely derived from that of its broadcaster. Besides, leveraging the trust certificates issued by ordinary vehicles generally cannot provide a strong robustness against the notorious collusion attack. Meanwhile, collecting trust recommendations from nearby reliable vehicles usually leads to a huge waste of bandwidth and time.

Data-Oriented: Raya *et al.* [30] proposed the notion of data trust and also came up with a novel data-centric trust (DCT) model for ephemeral ad hoc networks (e.g., VANETs). In their model, data trust is evaluated by leveraging multiple kinds of decision logics (e.g., Dempster–Shafer theory, weighted voting, Bayesian inference, etc.) based on several kinds of metrics on data itself (e.g., time freshness, location relevance, etc.), instead of its broadcaster. However, this article ignores the fact that entity-oriented trust is one of the significant sources of data-oriented trust. Huang *et al.* [35] identified the information oversampling issue in MV model [31] and proposed a novel CIO model for decision making in VANETs. In their model, each message is assigned a weight based on the minimum hop count from any one of the event witnesses to the broadcaster of this message. Besides, the authors showed that the CIO model achieves its best performance in the case that only taking the event witnesses' messages into account. However, their model also completely overlooks entity-oriented trust, and malicious vehicles can disguise themselves as event witnesses and other vehicles cannot effectively distinguish them from the actual event witnesses.

III. Trust Cascading and the TCEMD Model

In this section, we first analyze the motivations of this article, and then detail the proposal of trust cascading. Subsequently, we illustrate the primary elements in the TCEMD model, and then detail the formalized notations and definitions for ease of later illustration.

A. Motivations of Our Work

1) Incorporating the Entity-Oriented Trust Values Into Data-Oriented Trust Evaluation: As we mentioned earlier, malicious vehicles always try their utmost to broadcast unreal messages to deceive subsequent vehicles, while honest vehicles usually try their best to broadcast real messages. Thus, an honest vehicle's message is more likely to be reliable than that of a malicious vehicle. In other words, a vehicle's trust level can reflect the quality of its messages to some extent, so we incorporate the entity-oriented trust values into data-oriented trust evaluation efficiently in our model for the purpose of improving vehicles' correct decision percentage (marked as Pc).

2) Considering the Messages Reporting Distinct Statuses of Emergency Event Together: In VANETs, every emergency event (e.g., an obstacle at a certain spot, denoted as $\mathcal{E}$) has different statuses which change over time. The most typical statuses consist of two categories, namely, existence (e.g., the obstacle stays at its original spot, represented as $\mathcal{E}^+$) and extinction (e.g., the obstacle is cleared away from its original spot, illustrated as $\mathcal{E}^-$), and $\mathcal{E}^+$ status usually stays for a while and then changes to $\mathcal{E}^-$ status.

When $\mathcal{E}$ occurs and is in $\mathcal{E}^+$ status, honest witnesses (which witness $\mathcal{E}^+$) broadcast messages reporting $\mathcal{E}^+$ to inform subsequent vehicles of the current status of $\mathcal{E}$, while malicious witnesses (which witness $\mathcal{E}^+$) broadcast messages reporting $\mathcal{E}^-$ to deceive subsequent vehicles. When $\mathcal{E}$'s actual status changes to $\mathcal{E}^-$, honest witnesses (which witness $\mathcal{E}^-$) broadcast messages reporting $\mathcal{E}^-$ to inform subsequent vehicles of the new status of $\mathcal{E}$, while malicious witnesses (which witness $\mathcal{E}^-$) broadcast messages reporting $\mathcal{E}^+$ to deceive subsequent vehicles.

Therefore, a message receiver may receive several messages reporting $\mathcal{E}^+/\mathcal{E}^-$ during a period of time. It should be noted that $\mathcal{E}^+$ and $\mathcal{E}^-$ represent the different statuses of $\mathcal{E}$. That is, they reflect the different road conditions at the same spot, thus it is of importance to consider the messages reporting $\mathcal{E}^+/\mathcal{E}^-$ together to improve vehicles' correct decision percentage.

3) Considering as Many as Possible Messages From Distinct Broadcasters Together: As mentioned earlier, due to the complex road environment and limited perception and processing ability, even a honest vehicle may also broadcast unreal messages with a probability of p ($p \in (0, 1)$). Furthermore, the probability of a malicious vehicle broadcasting unreal messages is usually larger than p since it usually tries its utmost to broadcast unreal messages. For ease of illustration, we present a simple example, in which the probability of each vehicle broadcasting unreal messages is assumed to be p, and each message receiver makes a decision based on the classic MV strategy [31]. The correlativity between a message receiver's correct decision probability (marked as $\mathcal{P}$) and distinct message broadcasters' number considered in its decision process

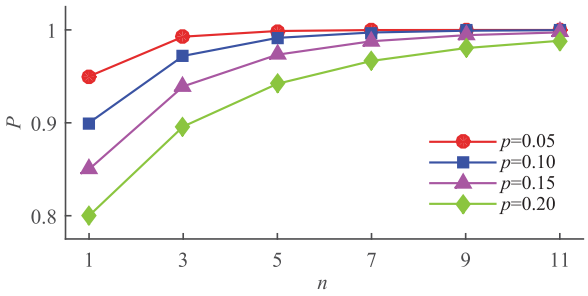


Fig. 2. Variation curves of $\mathcal{P}$ versus n when p takes different values.

(marked as n) can be derived as

$$\mathcal{P} = \sum_{i=\lceil \frac{n}{2} \rceil}^{n} C_n^i * (1-p)^i * p^{n-i} \tag{1}$$

and the variation curves of $\mathcal{P}$ versus n when p takes different values are shown in Fig. 2, which demonstrate that $\mathcal{P}$ generally increases with n when p takes 0.05, 0.10, ..., or 0.20.

From Fig. 2 and the above analysis, we can easily find the importance of considering as many as possible messages from different message broadcasters together. Furthermore, when a vehicle receives a message about an emergency event (marked as $\mathcal{E}$) for the first time, there is usually quite a distance between the vehicle and the location of $\mathcal{E}$, thus the vehicle is able to wait for more messages about $\mathcal{E}$, until it is close enough to $\mathcal{E}$'s location and has to make a decision immediately (the detailed discussion for decision trigger is provided in Section IV-D).

4) Utilizing Trust Certificate to Derive Entity-Oriented Trust Value: As we mentioned earlier, in classic infrastructure-based trust models, CA has to be available and accessible all the time to every vehicle, and requesting for a message broadcaster's latest trust value by a message receiver usually incurs relatively large time delay and limits the speed of trust evaluation and message dissemination. Moreover, due to the highly dynamic feature of VANETs, it is usually difficult for self-organized trust models to collect enough information for trust evaluation and provide high evaluation accuracy and robustness [26].

Utilizing the trust certificate can be understood as a tradeoff between infrastructure-based and self-organized trust models, and has some attractive advantages.

1) The trust certificate can be contained in the message to certify the trustworthiness of its broadcaster, and a message receiver can verify its authenticity by utilizing the digital signature technology and quickly derive the trust value of message broadcaster without the participation of CA.
2) The entity-oriented trust can be regularly updated by leveraging the periodical reissue of trust certificate.
3) Utilizing the trust certificate enables our model to have the failure tolerance feature in terms of the failure of a fraction of RSUs and temporary failure of CA.
4) Trust certificate can be efficiently integrated with digital signature and cryptography technologies for the purpose of achieving strong robustness against several kinds of attacks and malicious behaviors.

B. Proposal of Trust Cascading

In VANETs, the emergency messages can be disseminated among vehicles in a cascading manner [35]. That is, a vehicle's message can influence the decisions of its several subsequent vehicles (which are located behind it along the road and can receive its messages in a single-hop or multihop manner) and not limit to its successors (which are located behind it along the road and can receive its messages in a single-hop manner). Moreover, we argue that the source of influence power can be modeled as entity-oriented trust, instead of a constant in [35]. In other words, the higher trust value of a vehicle results in the higher influence power of its message, and vice versa. We name this proposal as *Trust Cascading* and denominate our model as the *Trust Cascading-Based Emergency Message Dissemination (TCEMD) model* which is quite distinct from the existing models, such as LT [36], MV [31], CIO [35], and RA [26] models.

1) LT model merely considers the influence of a single factor (e.g., a single status of $\mathcal{E}$, i.e., $\mathcal{E}^+$ or $\mathcal{E}^-$), while the TCEMD model considers the integrated influence of two kinds of typical statuses of $\mathcal{E}$ (i.e., $\mathcal{E}^+$ and $\mathcal{E}^-$).
2) MV and CIO models entirely ignore entity-oriented trust, while the TCEMD model efficiently incorporates the entity-oriented trust values into data-oriented trust evaluation.
3) RA model separately considers each message about $\mathcal{E}$ all the time, while the TCEMD model usually considers as many as possible messages reporting $\mathcal{E}^+/\mathcal{E}^-$ from different message broadcasters together.

As a result, the TCEMD model is able to primely overcome the deficiencies of LT, MV, CIO, and RA models, and the detailed theoretical performance analysis and simulational performance evaluation are provided in Sections V and VI, respectively.

C. Primary Elements in the TCEMD Model

The schematic diagram of the TCEMD model is shown in Fig. 3, in which there are three kinds of primary elements, namely, CA, RSUs, and vehicles.

1) CA: The TCEMD model contains a trusted CA which is tasked with admitting vehicles into and revoking vehicles from the VANET system, as well as storing and periodically updating vehicles' trust information based on the received trust feedbacks. When CA receives a request from a legal vehicle, it generates a new trust certificate at once based on the vehicle's latest trust information in its storage and sends it back to the vehicle with the aid of an available RSU. We assume that CA is equipped with a clock and secretly stores its private key, and its public key is known to all the vehicles. It should be noted that in the TCEMD model, CA is not needed to be available and accessible all the time (the concrete analysis is provided in Section V-B).

The justifications for adopting a centralized CA are summed up as follows.

1) It is in line with the practice that vehicles are generally managed by the traffic safety administration (TSA, which is a CA in nature), and makes our proposed model easy to manage, control, and protect.

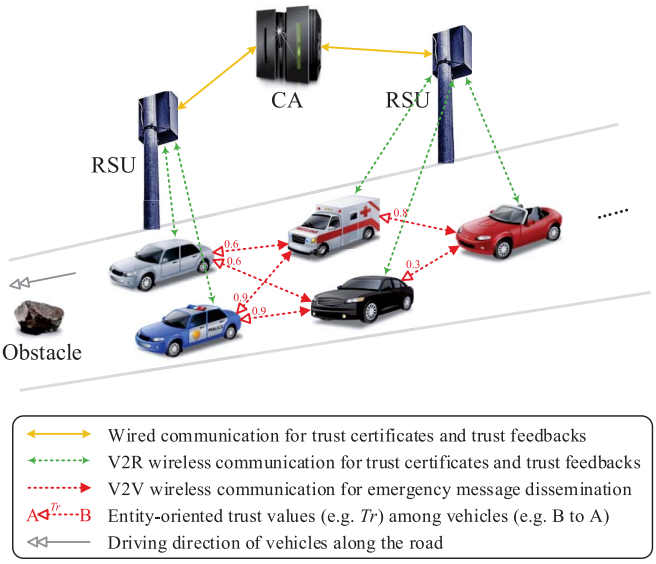


Fig. 3. Schematic of the TCEMD model.

2) It also makes our proposed model easy to effectively combine with some digital signature and cryptography technologies which generally contain a or a few CAs, and enables our model to provide strong robustness against several kinds of attacks and malicious behaviors.
3) Utilizing the trust certificates issued by CA enables our model to overcome the drawbacks of classic infrastructure-based models to a large extent.

2) RSUs: In the TCEMD model, RSUs are regarded to be installed along the side of road and serve as communication interfaces between vehicles and CA, and they generally connect to vehicles and CA through the V2R wireless communication and wired communication, respectively. It is worth noting that our model only requires public communication channels (instead of specific secure channels) between CA and RSUs, as it effectively combines with the cryptography technologies. Besides, in our model, it is not necessary that all the RSUs be available from beginning to end (the detailed analysis is shown in Section V-B).

3) Vehicles: In the TCEMD model, each vehicle is regarded to be equipped with an advanced global positioning system (GPS) or BeiDou system (BDS) that can obtain the accurate coordinates of both the vehicle itself and the emergency events which it witnesses, and an on-board unit (OBU) which can receive and broadcast messages from and to the OBUs on neighboring vehicles, so vehicles can communicate with each other in the V2V wireless manner so as to realize the emergency message dissemination. Each vehicle periodically requests for its latest trust certificate from CA when it is in the communication range of an available RSU. When an emergency event (marked as $\mathcal{E}$) takes place, the emergency messages about $\mathcal{E}$ can be disseminated among the nearby vehicles in a trust cascading manner, where the entity-oriented trust values can be derived from the trust certificates in the messages and then be adopted as important weights.

Moreover, we assume that each vehicle equips its OBU with a trusted hardware to securely store its private key, conduct the embedded digital signature and cryptography algorithms, and run a secure clock which is always in sync with that in CA.

D. Formalized Notations and Definitions

For the sake of later illustration, we present the formalized notations and definitions in the TCEMD model as follows.

1) $\mathcal{E}$, $\mathcal{E}^+$, $\mathcal{E}^-$: Emergency event (e.g., an obstacle at a certain spot), $\mathcal{E}$'s existence status (e.g., the obstacle stays at its original spot), and $\mathcal{E}$'s extinction status (e.g., the obstacle is cleared away from its original spot), respectively. Note that $\mathcal{E}$, $\mathcal{E}^+$, and $\mathcal{E}^-$ contain the same location information.
2) *Ve(i):* Vehicle whose unique identity is i.
3) *Pk(C), Sk(C), Pk(i), Sk(i):* CA's public key and private key, *Ve*(i)'s public key and private key, respectively.
4) $\mathcal{DS}$ = (KeyGen, Sign, Verify)*:* Digital signature algorithm, where KeyGen, Sign, Verify denote key generation, signature, and verify subalgorithms, respectively.
5) $\mathcal{BI}$, $\mathcal{TF}$*:* Basic information table and trust feedback table in CA's database, respectively.
6) *Tr(i): Ve*(i)'s entity-oriented trust value in $\mathcal{BI}$ table.
7) *HA, MA, and LA:* Sets of high-, medium-, low-authority-level vehicles, respectively.
8) Γ*:* Length of time interval for CA to update vehicles' trust information and for vehicles to request for their new trust certificates periodically.
9) Γ'*:* Threshold for determining whether a trust certificate is expired, where $\Gamma' > \Gamma$, and we define $\Delta\Gamma = \Gamma' - \Gamma$.
10) *Tc(i): Ve*(i)'s trust certificate which is issued by CA.
11) λ*:* Decay factor for updating vehicles' trust values periodically.
12) *Ms*($i, \mathcal{E}$)*:* Emergency message which is broadcasted by *Ve*(i) about $\mathcal{E}$.
13) Φ, Ψ, Ω, Θ*:* Thresholds for judging whether an emergency message is expired, whether a trust feedback is timely, whether a trust feedback record is available, and whether a vehicle should be revoked, respectively.
14) *Mw, Md, Mi:* Maximum witness, decision, and influence distances along the road, respectively.
15) *Ds*($i, \mathcal{E}$)*: Ve*(i)'s distance to the location of $\mathcal{E}$ along the road.
16) *MS*($i, \mathcal{E}$)*:* Set of emergency messages about $\mathcal{E}$ stored by *Ve*(i) in its local storage.
17) *Dt*($i, \mathcal{E}$)*:* $\mathcal{E}$'s trust value derived by *Ve*(i).
18) *Tp(C), Tp(i):* Trust parameters determined by CA and *Ve*(i), respectively.
19) *TF*($i, \mathcal{E}$)*:* Trust feedback set reported by *Ve*(i) about $\mathcal{E}$.
20) *VC(i):* Set of vehicles which collude with *Ve*(i).
21) *VN:* Set of vehicles which are not revoked by CA.

Definition 1 (Witness): If a vehicle witnesses $\mathcal{E}^+/\mathcal{E}^-$, it is called as $\mathcal{E}$'s witness.

Definition 2 (Follower): If a vehicle is located behind $\mathcal{E}$'s witnesses along the road and does not witness $\mathcal{E}^+/\mathcal{E}^-$, it is named as $\mathcal{E}$'s follower.

Definition 3 (Precursor): If a vehicle is in front of *Ve*(i) along the road and broadcasts messages reporting $\mathcal{E}^+/\mathcal{E}^-$ to

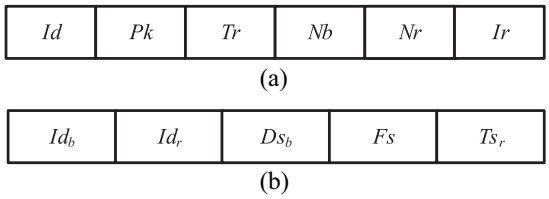


Fig. 4. Structure of (a) $\mathcal{BI}$ and (b) $\mathcal{TF}$ tables.

$Ve(i)$ in a single-hop manner, it is named as $Ve(i)$'s precursor about $\mathcal{E}$.

Definition 4 (Successor): If a vehicle is in back of $Ve(i)$ along the road and receives $Ve(i)$'s messages reporting $\mathcal{E}^+/\mathcal{E}^-$ in a single-hop manner, it is referred to as $Ve(i)$'s successor about $\mathcal{E}$.

Definition 5 (Subsequent Vehicle): If a vehicle is in back of $Ve(i)$ along the road and receives $Ve(i)$'s messages reporting $\mathcal{E}^+/\mathcal{E}^-$ in a single-hop or multihop manner, it is called as $Ve(i)$'s subsequent vehicle about $\mathcal{E}$.

IV. Stages in the TCEMD Model

In this section, we detail concrete stages in the TCEMD model, namely, the initialization of CA and RSUs, vehicle registration, trust certificate requesting, emergency message dissemination, trust feedback reporting, trust information updating, and vehicle revocation.

A. Initialization of CA and RSUs

1) Initialization of CA: When the TCEMD model is deployed in a VANET system, CA first installs $\mathcal{DS}$ = (KeyGen, Sign, Verify) algorithm, and then sets its clock and generates its public key $Pk(C)$ and private key $Sk(C)$ by leveraging KeyGen subalgorithm, where $Sk(C)$ is remained strictly confidential all the time. Moreover, to secretly store the information of every vehicle, CA creates a database which contains two tables, namely, basic information table and trust feedback table (denoted as $\mathcal{BI}$ and $\mathcal{TF}$ tables, respectively).

The structure of $\mathcal{BI}$ table is illustrated as Fig. 4(a), which is composed of six fields, namely, vehicle's identity Id, public key Pk, latest trust value Tr, number of broadcasting emergency messages Nb, number of reporting trust feedbacks Nr, and indicator of being revoked or not Ir.

The structure of $\mathcal{TF}$ table is illustrated as Fig. 4(b), which consists of five fields, namely, identity of message broadcaster Id_b, identity of feedback reporter Id_r, digital signature in the message Ds_b, feedback score about the message Fs, and timestamp of when the trust feedback is generated Ts_r.

2) Initialization of RSUs: In the TCEMD model, when a new RSU is installed on the side of road or a broken RSU is substituted by a new one, a public wired communication channel between the new RSU and CA should be constructed, and then the new RSU also becomes a communication interface between vehicles and CA.

B. Vehicle Registration

When a new vehicle registers with the VANET system, CA first assigns it a unique identity (e.g., i), then the new vehicle can be denoted as $Ve(i)$ for ease of illustration. Furthermore, CA generates the public key $Pk(i)$ and private key $Sk(i)$ for $Ve(i)$ by utilizing KeyGen subalgorithm, and equips $Ve(i)$'s OBU with a trusted hardware which can securely store $Sk(i)$ and conduct Sign subalgorithm, as well as run a secure clock which is always in sync with that in CA. Besides, CA installs Verify subalgorithm and $Pk(C)$ into $Ve(i)$'s OBU. It should be added that it is not necessary to install them into $Ve(i)$'s trusted hardware.

Moreover, CA inserts a new record for $Ve(i)$ into $\mathcal{BI}$ table, where the values of Id and Pk fields are set as i and $Pk(i)$, respectively, and the values of other fields [denoted as $Tr(i)$, $Nb(i)$, $Nr(i)$, $Ir(i)$, respectively] can be derived based on the following analysis.

As we well know, there are distinct kinds of vehicles in the VANET system, such as patrol car, taxi, bus, private car, and so on. Based on authority level, we can divide them into three categories, namely, high-authority-level vehicles which refer to law enforcement vehicles (e.g., patrol car), medium-authority-level vehicles which refer to public service vehicles (e.g., taxi, bus, ambulance, etc.) which are generally managed by specific departments, and low-authority-level vehicles referring to the other vehicles which are controlled by individuals (e.g., private car). Inspired by the work of Yao *et al.* [34] in our proposed model, CA can derive the initial value of $Tr(i)$ as

$$Tr(i) = \begin{cases} 0.9, & \text{if } Ve(i) \in HA \\ 0.5, & \text{if } Ve(i) \in MA \\ 0.1, & \text{if } Ve(i) \in LA \end{cases} \tag{2}$$

where HA, MA, and LA denote the sets of high-, medium-, and low-authority-level vehicles, respectively.

Furthermore, as a newly registered vehicle, $Ve(i)$ has never broadcasted emergency messages or reported trust feedbacks and it is not revoked by CA, thus the initial values of $Nb(i)$, $Nr(i)$, and $Ir(i)$ are set as 0, 0, and FALSE, respectively.

C. Trust Certificate Requesting

When a vehicle (e.g., $Ve(i)$) is in the communication range of any available RSU, it can request for its new trust certificate from CA at the interval of Γ ($\Gamma > 0$). In particular, it sends its identity i to CA via the RSU, then CA generates a new trust certificate $Tc(i)$ for $Ve(i)$ according to the trust information in $\mathcal{BI}$ table if $Ve(i)$ is not revoked (i.e., $Ir(i)$ = FALSE), and the concrete format of $Tc(i)$ is

$$Tc(i) = (i, Pk(i), Tr(i), Ts_C(i), Ds_C(i)) \tag{3}$$

where $Ts_C(i)$ denotes the timestamp (which can be obtained from CA's clock) of when $Tc(i)$ is generated, and

$$Ds_C(i) = \text{Sign}(i, Pk(i), Tr(i), Ts_C(i))_{Sk(C)} \tag{4}$$

represents the digital signature which is signed by CA through utilizing Sign subalgorithm and $Sk(C)$ on the first four parts of $Tc(i)$.

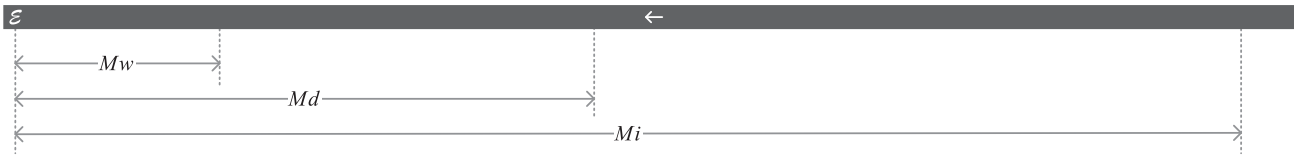


Fig. 5. Three kinds of distances (i.e., maximum witness distance *Mw*, maximum decision distance *Md*, and maximum influence distance *Mi*) for a one-way straight road, where $\mathcal{E}$ represents an emergency event and the arrow denotes the driving direction of vehicles along the road.

Subsequently, CA sends $Tc(i)$ to $Ve(i)$ via the RSU, then $Ve(i)$ stores it in its local storage and substitutes the old one. In addition, if $Ve(i)$ does not receive $Tc(i)$, it tries to request for its new trust certificate from CA again once it drives into the communication range of another available RSU.

It's worth noting that in the above process, the request message (i.e., i) does not adopt any digital signature, and the request message and the response message (i.e., $Tc(i)$) are transmitted without encryption, as it is useless for each vehicle to acquire other vehicles' trust certificates (the detailed analysis is shown in Section V-A). In addition, as CA updates vehicles' trust information periodically (i.e., at the interval of Γ), $Ve(i)$ does not need to request for new trust certificate whenever it drives into the communication range of an available RSU. Instead, it merely needs to do so at the interval of Γ.

D. Emergency Message Dissemination

In the TCEMD model, when an emergency event (i.e., $\mathcal{E}$) occurs, the emergency messages reporting $\mathcal{E}$'s different statuses (i.e., $\mathcal{E}^+/\mathcal{E}^-$) can be disseminated among nearby vehicles, and the specific format of emergency message about $\mathcal{E}$ broadcasted by $Ve(i)$ is

$$Ms(i,\mathcal{E}) = (Tc(i), Mc(i,\mathcal{E}), Ts_b(i,\mathcal{E}), Ds_b(i,\mathcal{E})) \tag{5}$$

where $Mc(i,\mathcal{E}) = \mathcal{E}^+/\mathcal{E}^-$ denotes $\mathcal{E}$'s status, $Ts_b(i,\mathcal{E})$ represents the timestamp [that can be obtained from the secure clock on $Ve(i)$'s trusted hardware] of when $Ms(i,\mathcal{E})$ is generated, and

$$Ds_b(i,\mathcal{E}) = \mathrm{Sign}(Mc(i,\mathcal{E}), Ts_b(i,\mathcal{E}))_{Sk(i)} \tag{6}$$

indicates the digital signature, that is signed by $Ve(i)$'s trusted hardware through leveraging Sign subalgorithm and $Sk(i)$ on $(Mc(i,\mathcal{E}), Ts_b(i,\mathcal{E}))$. In this stage, the trusted hardware ensures that $Ve(i)$ cannot tamper with $Ts_b(i,\mathcal{E})$ and both $Ve(i)$ and other vehicles cannot acquire $Sk(i)$.

When $\mathcal{E}$ is in $\mathcal{E}^+$ status, all the witnesses trust $\mathcal{E}^+$, since they witness it. Furthermore, honest witnesses promptly broadcast emergency messages reporting $\mathcal{E}^+$ [i.e., $Mc(i,\mathcal{E}) = \mathcal{E}^+$, the same below] to inform subsequent vehicles of $\mathcal{E}$'s current status (i.e., $\mathcal{E}^+$), while malicious witnesses broadcast emergency messages reporting $\mathcal{E}^-$ [i.e., $Mc(i,\mathcal{E}) = \mathcal{E}^-$, the same below] to deceive subsequent vehicles.

When $\mathcal{E}$'s status changes to $\mathcal{E}^-$, all the witnesses trust $\mathcal{E}^-$. Moreover, honest witnesses immediately broadcast emergency messages reporting $\mathcal{E}^-$ to inform subsequent vehicles of $\mathcal{E}$'s updated status (i.e., $\mathcal{E}^-$), while malicious witnesses broadcast emergency messages reporting $\mathcal{E}^+$ so as to deceive subsequent vehicles.

The case for followers is relatively complicated, as they do not witness $\mathcal{E}^+/\mathcal{E}^-$ and have to make decisions based on their precursors' messages. As we analyzed in Section III-A, to improve the correct decision probability, every follower should consider as many as possible messages reporting $\mathcal{E}^+/\mathcal{E}^-$ from different precursors before making a comprehensive decision. The setting of decision trigger is an interesting issue.

1) If a follower makes a decision too early, it is merely able to consider few messages reporting $\mathcal{E}^+/\mathcal{E}^-$ from different precursors, and $\mathcal{E}$'s status may change with it moving toward the location of $\mathcal{E}$, thus the follower's decision may be one-sided and has a low correct probability.
2) If a follower makes a decision too late, it may have great difficulty in taking corresponding actions and broadcasting messages reporting $\mathcal{E}^+/\mathcal{E}^-$ to subsequent vehicles in time, since it is already too close to the location of $\mathcal{E}$. In this case, the decision making does not make much sense even if its result is exactly correct.

Hence, the setting of decision trigger is a tradeoff between correct decision probability and decision timeliness. Inspired by the study of Ostermaier *et al.* [31], we presented three kinds of distances (i.e., maximum witness distance *Mw*, maximum decision distance *Md*, and maximum influence distance *Mi*) for a one-way straight road (For a complicated road, *Mw*, *Md*, and *Mi* can also be derived with the aid of digital map [49], and the details are beyond the scope of this article) as revealed in Fig. 5, where $Mw < Md < Mi$. If $Ve(i)$'s distance to the location of $\mathcal{E}$ along the road (i.e., $Ds(i,\mathcal{E})$) satisfies $Ds(i,\mathcal{E}) \in [0, Mw]$, it is a witness of $\mathcal{E}$. Otherwise [i.e., if $Ds(i,\mathcal{E}) \in (Mw, +\infty)$], it is a follower of $\mathcal{E}$.

When a follower (e.g., $Ve(j)$) receives an emergency message $Ms(i,\mathcal{E})$ about $\mathcal{E}$ from its precursor $Ve(i)$, it first extracts $Tc(i)$ and verifies $Ds_C(i)$ by leveraging Verify subalgorithm and $Pk(C)$ that are stored in $Ve(j)$'s OBU, and then extracts $Ts_C(i)$ from $Tc(i)$ and gets the current timestamp Ts_n from the secure clock to verify $Ts_n - Ts_C(i) \le \Gamma'$ (i.e., check whether $Tc(i)$ is expired). Furthermore, $Ve(j)$ extracts $Pk(i)$ from $Tc(i)$ and verifies $Ds_b(i,\mathcal{E})$ by utilizing Verify subalgorithm and $Pk(i)$, and then verifies $Ts_n - Ts_b(i,\mathcal{E}) \le \Phi$ [i.e., checks whether $Ms(i,\mathcal{E})$ is expired].

If any of these verifications fails, $Ve(i)$ regards $Ms(i,\mathcal{E})$ as illegal and directly discards it. Otherwise, $Ve(j)$ extracts the locations of $\mathcal{E}$ from $Mc(i,\mathcal{E})$ and of its own from its GPS or BDS, and then calculates its distance to the location of $\mathcal{E}$ along the road (i.e., $Ds(j,\mathcal{E})$) and takes corresponding strategies.

1) If $Ve(j)$ is far from $\mathcal{E}$'s location (i.e., $Ds(j,\mathcal{E}) \in (Mi, +\infty)$), it directly disregards $Ms(i,\mathcal{E})$ as it is outside $\mathcal{E}$'s influence area.

2) When $Ve(j)$ moves closer to $\mathcal{E}$'s location (i.e., $Ds(j, \mathcal{E}) \in (Md, Mi]$), it adds $Ms(i, \mathcal{E})$ to the set of emergency messages about $\mathcal{E}$ (i.e., $MS(j, \mathcal{E})$) in its local storage, but it do not rush to make a decision. Furthermore, if $Ve(j)$ receives multiple messages from the same precursor, it merely stores the latest one.
3) When $Ve(j)$ moves to the neighborhood of $\mathcal{E}$'s location (i.e., $Ds(j, \mathcal{E}) \in (Mw, Md]$), it makes a decision at once based on the messages in $MS(j, \mathcal{E})$.

In concrete terms, $Ve(j)$ first derive $\mathcal{E}$'s trust value $Dt(j, \mathcal{E})$ as

$$Dt(j, \mathcal{E}) = \frac{\sum_{Ms(i,\mathcal{E}) \in MS(j,\mathcal{E})} Mc'(i, \mathcal{E}) * Tr(i)}{\sum_{Ms(i,\mathcal{E}) \in MS(j,\mathcal{E})} Tr(i)} \tag{7}$$

where $Mc'(i, \mathcal{E})$ can be converted from $Mc(i, \mathcal{E})$ as

$$Mc'(i, \mathcal{E}) = \begin{cases} 1, & \text{if } Mc(i, \mathcal{E}) = \mathcal{E}^+ \\ -1, & \text{if } Mc(i, \mathcal{E}) = \mathcal{E}^- \end{cases} \tag{8}$$

and $Tr(i)$ denotes $Ve(i)$'s entity-oriented trust value in $Tc(i)$.

As $Tr(i) \in [0, 1]$ and $Mc'(i, \mathcal{E}) = \pm 1$, it is notable that $Dt(j, \mathcal{E})$ falls into the of $[-1, 1]$. Furthermore, from (7), we can easily discover that $Tr(i)$ is adopted as a significant weight in $Dt(j, \mathcal{E})$'s calculation process. In other words, the entity-oriented trust values are incorporated into data-oriented trust evaluation in an efficient manner.

Subsequently, $Ve(j)$ can make a decision based on $Dt(j, \mathcal{E})$ and its trust parameter $Tp(j) \in [0, 1]$ as follows.

1) If $Dt(j, \mathcal{E}) \in [Tp(j), 1]$, $Ve(j)$ trusts $\mathcal{E}^+$ and takes action on $\mathcal{E}^+$ at once (e.g., reduces the driving speed). Moreover, if it is honest, it broadcasts a new message $Ms(j, \mathcal{E})$ in which $Mc(j, \mathcal{E}) = \mathcal{E}^+$ to inform subsequent vehicles, and if it is malicious, it broadcasts the message $Ms(j, \mathcal{E})$ in which $Mc(j, \mathcal{E}) = \mathcal{E}^-$ to deceive subsequent vehicles.
2) If $Dt(j, \mathcal{E}) \in [-1, -Tp(j)]$, $Ve(j)$ trusts $\mathcal{E}^-$, and it takes immediate action on $\mathcal{E}^-$ (e.g., restores the driving speed). Furthermore, if it is honest, it broadcasts a new message $Ms(j, \mathcal{E})$ in which $Mc(j, \mathcal{E}) = \mathcal{E}^-$ to inform subsequent vehicles, and if it is malicious, it broadcasts the message $Ms(j, \mathcal{E})$ in which $Mc(j, \mathcal{E}) = \mathcal{E}^+$ to deceive subsequent vehicles.
3) If $Dt(j, \mathcal{E}) \in (0, Tp(j))$, $Ve(j)$ trusts $\mathcal{E}^+$ to some degree, thus it takes action on $\mathcal{E}^+$ at once but does not broadcast its own message to subsequent vehicles.
4) If $Dt(j, \mathcal{E}) \in (-Tp(j), 0]$, $Ve(j)$ trusts $\mathcal{E}^-$ to a certain extent, thus it takes immediate action on $\mathcal{E}^-$ but does not broadcast its own message to subsequent vehicles.

It is very remarkable that in the TCEMD model, every follower (e.g., $Ve(j)$) does not relay precursors' messages and merely broadcasts its own message (after making a decision based on precursors' messages) if it is quite sure about $\mathcal{E}$'s status (i.e., $|Dt(j, \mathcal{E})| \geq Tp(j)$), for the purpose of decreasing the number of negative trust feedbacks from message receivers because of broadcasting uncertain messages. These strategies can limit the dissemination of unreal or uncertain messages and reduce the total number of emergency messages in the VANET system as well as relieve the wireless channel collision problem [5], [14] to some extent (the concrete verification is shown in Section VI).

E. Trust Feedback Reporting

When a follower $Ve(j)$ moves to the neighborhood of $\mathcal{E}$'s location so that $Ds(j, \mathcal{E}) \in [0, Mw]$, it can perceive $\mathcal{E}$'s actual status (marked as $As(j, \mathcal{E}) \in \{\mathcal{E}^+, \mathcal{E}^-\}$). Besides, if $As(j, \mathcal{E})$ is not consistent with that it has reported, $Ve(j)$ broadcasts a new message (where if $Ve(j)$ is honest, $Mc(i, \mathcal{E}) = As(j, \mathcal{E})$, otherwise, $Mc(i, \mathcal{E}) = \neg As(j, \mathcal{E})$) to subsequent vehicles.

Moreover, $Ve(j)$ can evaluate the quality of every message in $MS(j, \mathcal{E})$. In concrete terms, it first calculates the feedback score $Fs(i, j, \mathcal{E})$ for $\forall Ms(i, \mathcal{E}) \in MS(j, \mathcal{E})$ as

$$Fs(i, j, \mathcal{E}) = \begin{cases} 1, & \text{if } As(j, \mathcal{E}) = Mc(i, \mathcal{E}) \\ 0, & \text{otherwise} \end{cases} \tag{9}$$

and generates the trust feedback $Tf(i, j, \mathcal{E})$ for $\forall Ms(i, \mathcal{E}) \in MS(j, \mathcal{E})$ as

$$\begin{aligned} Tf(i, j, \mathcal{E}) = (i, Fs(i, j, \mathcal{E}), Mc(i, \mathcal{E}) \\ Ts_b(i, \mathcal{E}), Ds_b(i, \mathcal{E})) \end{aligned} \tag{10}$$

where i denotes the identity of emergency message broadcaster, and $Mc(i, \mathcal{E})$, $Ts_b(i, \mathcal{E})$, and $Ds_b(i, \mathcal{E})$ are the elements of $Ms(i, \mathcal{E})$. For ease of illustration, $Tf(i, j, \mathcal{E})$ can be called as a positive trust feedback if $Fs(i, j, \mathcal{E}) = 1$ and as a negative trust feedback if $Fs(i, j, \mathcal{E}) = 0$.

Next, $Ve(j)$ can construct the trust feedback set $TF(j, \mathcal{E})$ for $\mathcal{E}$ as

$$\begin{aligned} TF(j, \mathcal{E}) = (j, \{Tf(i, j, \mathcal{E}) | \forall Ms(i, \mathcal{E}) \in MS(j, \mathcal{E})\} \\ Ts_r(j, \mathcal{E}), Ds_r(j, \mathcal{E})) \end{aligned} \tag{11}$$

where j indicates the identity of feedback reporter, $Ts_r(j, \mathcal{E})$ represents the timestamp [which can be obtained from the secure clock run on $Ve(j)$'s trusted hardware] of when $TF(j, \mathcal{E})$ is constructed, and

$$\begin{aligned} Ds_r(j, \mathcal{E}) = \text{Sign}(j, \{Tf(i, j, \mathcal{E}) | \forall Ms(i, \mathcal{E}) \in \\ MS(j, \mathcal{E})\}, Ts_r(j, \mathcal{E}))_{Sk(j)} \end{aligned} \tag{12}$$

indicates the digital signature, that is signed by $Ve(j)$'s trusted hardware through adopting Sign subalgorithm and $Sk(j)$ on the first three parts of $TF(j, \mathcal{E})$. In the above procedure, the trusted hardware ensures that $Ve(j)$ cannot modify $Ts_r(j, \mathcal{E})$ and both $Ve(j)$ and other vehicles cannot acquire $Sk(j)$.

Subsequently, $Ve(j)$ stores $TF(j, \mathcal{E})$ in its local storage and then reports it to CA via an available RSU when it drives into the RSU's communication range. It should be noted that $Ve(j)$ will not delete $TF(j, \mathcal{E})$ from its local storage before receiving CA's acknowledgment.

It is worth noting that in the TCEMD model, the trust feedbacks for all the messages about the same emergency event (e.g., $\mathcal{E}$) are packaged before being signed and sent to CA, as revealed in (10)–(12). The major justifications are as follows: 1) when a follower perceives the actual status of an emergency event, it can evaluate the quality of all the messages about the same emergency event and generate trust feedbacks for them almost simultaneously and 2) packaging the trust feedbacks before signing and sending can reduce the consumption of computing resource by limiting the count of conducting Sign and Verify subalgorithms and of wireless bandwidth resource by reducing the total number and total data size of trust feedbacks.

Furthermore, in this stage, a malicious vehicle (e.g., $Ve(j)$) may deliberately inflate the trust values of vehicles that collude with it [the set is represented as $VC(j)$] and deflates the trust values of other vehicles by modifying (9) to

$$Fs(i,j,\mathcal{E}) = \begin{cases} 1, & \text{if } Ve(i) \in VC(j) \\ 0, & \text{otherwise} \end{cases} \tag{13}$$

and the corresponding mitigation strategies in the TCEMD model are presented in the next section.

F. Trust Information Updating

Whenever CA receives a signed trust feedback set $TF(j,\mathcal{E})$ about $\mathcal{E}$ from $Ve(j)$, it first extracts $Ve(j)$'s unique identity j and retrieves $Ir(j)$ and $Pk(j)$ from $\mathcal{BI}$ table, then checks whether $Ir(j) =$ FALSE, and verifies $Ds_r(j,\mathcal{E})$ by leveraging Verify subalgorithm and $Pk(j)$. If the retrieval, check, or verification fails, CA considers $TF(j,\mathcal{E})$ as illegal and directly discards it. Otherwise, CA obtains the current timestamp $Ts_{n'}$ from its clock and extracts trust feedbacks from $TF(j,\mathcal{E})$, and verifies each of them (e.g., $Tf(i,j,\mathcal{E})$) as follows: 1) it extracts $Ve(i)$'s unique identity i and retrieves $Pk(i)$ from $\mathcal{BI}$ table, and verifies $Ds_b(i,\mathcal{E})$ by leveraging Verify subalgorithm and $Pk(i)$; 2) it verifies $i \neq j$ [i.e., checks whether $Ve(j)$ praises itself]; 3) it verifies $Ir(i) =$ FALSE in $\mathcal{BI}$ table [i.e., checks whether $Ve(i)$ is revoked]; 4) it verifies $Ts_{n'} - Ts_b(i,\mathcal{E}) \leq \Psi$ [i.e., checks whether $Tf(i,j,\mathcal{E})$ is timely enough]; and 5) it verifies $Fs(i,j,\mathcal{E}) \in \{0, 1\}$ [i.e., checks whether $Fs(i,j,\mathcal{E})$'s value is in accordance with (9)]. If any of 1)–5) fails, $Tf(i,j,\mathcal{E})$ is viewed as illegal and discarded by CA. Otherwise, CA inserts a new record into $\mathcal{TF}$ table for $Tf(i,j,\mathcal{E})$, in which the values of all the fields are i, j, $Ds_b(i,\mathcal{E})$, $Fs(i,j,\mathcal{E})$, and $Ts_r(j,\mathcal{E})$, respectively. At the same time, if there exists a previous record that has the same values in Id_b, Id_r, Ds_b fields with the newly inserted record, CA deletes the previous one.

Subsequently, CA generates an acknowledgment $Ac(j,\mathcal{E})$ and sends it to $Ve(j)$ via the RSU for the purpose of informing $Ve(j)$ that CA has received $TF(j,\mathcal{E})$. The concrete format of $Ac(j,\mathcal{E})$ is

$$Ac(j,\mathcal{E}) = (j, Ds_r(j,\mathcal{E}), Ds_{C'}(j,\mathcal{E})) \tag{14}$$

where $Ds_r(j,\mathcal{E})$ is the digital signature in $TF(j,\mathcal{E})$ and

$$Ds_{C'}(j,\mathcal{E}) = \text{Sign}(j, Ds_r(j,\mathcal{E}))_{Sk(C)} \tag{15}$$

represents the digital signature signed by CA through utilizing Sign subalgorithm and $Sk(C)$ on $(j, Ds_r(j,\mathcal{E}))$.

After receiving $Ac(j,\mathcal{E})$, $Ve(j)$ first verifies $Ds_{C'}(j,\mathcal{E})$ by leveraging Verify subalgorithm and $Pk(C)$ which are stored in its OBU, and then it extracts $Ds_r(j,\mathcal{E})$ from $Ac(j,\mathcal{E})$ and verifies that it is identical to $Ds_r(j,\mathcal{E})$ in $TF(j,\mathcal{E})$ (which is still stored in its local storage). If these verifications succeed, $Ve(j)$ considers that CA has received $TF(j,\mathcal{E})$, thus it deletes $TF(j,\mathcal{E})$ from its local storage. Otherwise, $Ve(j)$ tries to send $TF(j,\mathcal{E})$ to CA again once it drives into the communication range of another available RSU.

Furthermore, CA iteratively updates the trust information of all the vehicles which are not revoked in $\mathcal{BI}$ table (The set is indicated as VN) based on the trust feedback records in $\mathcal{TF}$ table at the interval of Γ. In concrete terms, CA first counts the total numbers of $\forall Ve(i) \in VN$ broadcasting emergency messages (i.e., $Nb(i)$) and reporting trust feedbacks (i.e., $Nr(i)$) within the time period of $[Ts_{n'} - \Omega, Ts_{n'}]$ (where Ω is a threshold to ensure that there are sufficient available trust feedbacks for the vast majority of vehicles) in $\mathcal{TF}$ table as

$$Nb(i) = |\{< Id_b, Id_r, Ds_b > | Id_b = i, Ts_{n'} - Ts_r \leq \Omega\}| \tag{16}$$

$$Nr(i) = |\{< Id_b, Id_r, Ds_b > | Id_r = i, Ts_{n'} - Ts_r \leq \Omega\}| \tag{17}$$

respectively, (where $||$ denotes the number of elements in a set, the same below), and then updates Nb and Nr fields' values of $\forall Ve(i) \in VN$ in $\mathcal{BI}$ table. Moreover, CA sorts $\forall Ve(i) \in VN$ in the descending order of $Nb(i)$ and $Nr(i)$, and obtains two sequences (indicated as SB and SR), respectively. Let $Sb(i)$ and $Sr(i)$ denote the sequence numbers of $\forall Ve(i) \in VN$ in SB and SR, respectively, in which $Sb(i), Sr(i) = 1, 2, \ldots,$ or $|VN|$. Besides, CA can derive the weights $Wb(i)$ and $Wr(i)$ corresponding to $Sb(i)$ and $Sr(i)$ for $\forall Ve(i) \in VN$ as

$$Wb(i) = \begin{cases} 1, & \text{if } Sb(i) \leq \frac{|VN|}{2} \\ \frac{3}{2} - \frac{Sb(i)}{|VN|}, & \text{otherwise} \end{cases} \tag{18}$$

$$Wr(i) = \begin{cases} 1, & \text{if } Sr(i) \leq \frac{|VN|}{2} \\ \frac{3}{2} - \frac{Sr(i)}{|VN|}, & \text{otherwise} \end{cases} \tag{19}$$

respectively. The variation curves of $Wb(i)$ versus $Sb(i)$ and of $Wr(i)$ versus $Sr(i)$ when $|VN| = 2k-1$ or $|VN| = 2k$ (where $k \in Z_+$) are intuitively illustrated in Fig. 6. From (18), (19), and Fig. 6, we can easily discover that the ranges of both $Wb(i)$ and $Wr(i)$ are [0.5, 1].

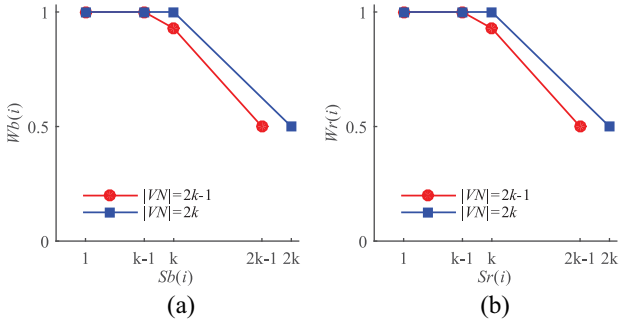


Fig. 6. Variation curves of (a) $Wb(i)$ versus $Sb(i)$ and of (b) $Wr(i)$ versus $Sr(i)$ when $|VN| = 2k-1$ or $|VN| = 2k$ (in which $k \in Z_+$).

Besides, CA can obtain the feedback reporter set $FS(i)$ and three-tuple set $TT(i)$ for $\forall Ve(i) \in VN$ from $\mathcal{TF}$ table as

$$FS(i) = \{Id_r | Id_b = i, Ts_{n'} - Ts_r \leq \Omega\} \cap \{j | Ve(j) \in VN\} \tag{20}$$

$$TT(i) = \{< Id_r, Ds_b, Fs > | Id_b = i,\ Id_r \in FS(i)\ Ts_{n'} - Ts_r \leq \Omega\} \tag{21}$$

respectively, and then calculate the new trust value $Tr_n(i)$ for $\forall Ve(i) \in VN$ as illustrated in (22), as shown at the bottom of the next page, in which $Tr(i)$ denotes $Ve(i)$'s current trust value in $\mathcal{BI}$ table, $\lambda \in (0, 1)$ indicates a decay factor determined by CA, and

$$Tt(i,j,\mathcal{E}) = <j, Ds_b(i,\mathcal{E}), Fs(i,j,\mathcal{E})> \tag{23}$$

is $TT(i)$'s element. That is, if

$$\sum\nolimits_{Tt(i,j,\mathcal{E})\in TT(i)} Tr(j) > 0 \tag{24}$$

holds, $Tr_n(i)$ is derived as the product of $(Wb(i) + Wr(i))/2$ and weighted average value of $Fs(i, j, \mathcal{E})$, where the trust values of feedback reporters are leveraged as important weights. Otherwise, $Tr_n(i)$ is derived as the product of a decay factor and $Ve(i)$'s current trust value in $\mathcal{BI}$ table. Next, CA updates the value of Tr field with $Tr_n(i)$ for $\forall Ve(i) \in VN$ in $\mathcal{BI}$ table. Besides, we can easily find that the range of $Tr_n(i)$ is [0, 1] from (22).

G. Vehicle Revocation

Whenever CA finishes the trust information updating in the previous stage, it computes the total number of negative trust feedbacks $Nn(i)$ from distinct feedback reporters in $\mathcal{TF}$ table for $\forall Ve(i) \in VN$ as

$$Nn(i) = |\{Id_r | Id_b = i,\ Id_r \in FS(i),\ Fs = 0 \\ Ts_{n'} - Ts_r \le \Omega\}| \tag{25}$$

and obtains the latest trust value $Tr(i)$ of $\forall Ve(i) \in VN$ from $\mathcal{BI}$ table. If $Tr(i) < Tp(C)$, where $\Theta \in Z_+$, $Tp(C) \in (0, 1)$ are parameters determined by CA, CA revokes $Ve(i)$ from the revokes $Ve(i)$ from the VANET system by updating its Ir field's value in $\mathcal{BI}$ table with TRUE [i.e., setting $Ir(i) =$ TRUE]. Subsequently, CA no longer generates any new trust certificate for $Ve(i)$ or updates $Ve(i)$'s trust information in $\mathcal{BI}$ table, and it disregards all the trust feedbacks reported by $Ve(i)$. Moreover, $Ve(i)$ can be entirely revoked from the VANET system when its existing trust certificate expires (i.e., $Ts_n - Ts_C(i) > \Gamma'$).

V. Performance Analysis

In this section, we analyze the robustness of the TCEMD model against several kinds of attacks and malicious behaviors, failure tolerance features, compatibility for several kinds of special situations, and incentive mechanisms in the TCEMD model.

A. Robustness Analysis

In the TCEMD model, the attacks can be broadly classified into the following two categories.

1) *External Attack:* Malicious vehicles which do not register with CA (named as external adversaries) attack the TCEMD model.
2) *Internal Attack:* Malicious vehicles that have legal identities (called as internal adversaries) attack the TCEMD model.

Furthermore, in each kind of attack, malicious vehicles may conduct the following two kinds of malicious behaviors.

1) *Broadcasting Unreal Emergency Messages (BUEM):* Malicious vehicles try their utmost to broadcast unreal emergency messages to deceive subsequent vehicles.
2) *Reporting Unfair Trust Feedbacks (RUTF):* Malicious vehicles try their utmost to report unfair trust feedbacks to CA for inflating/deflating other vehicles' trust values. It is worth noting that the main purpose of malicious vehicles taking RUTF behavior is usually to be able to take BUEM behavior for a longer time before being revoked by CA.

Next, we analyze the robustness of the TCEMD model against different malicious behaviors in two kinds of attacks in detail, respectively.

1) BUEM Behavior in External Attack: In our model, an external adversary may adopt the following strategies to take BUEM behavior: 1) it tampers with a message $Ms(i, \mathcal{E})$ of a legal vehicle (e.g., $Ve(i)$) through modifying $Mc(i, \mathcal{E})$; 2) it requests for a trust certificate $Tc(i)$ from CA in the name of a legal vehicle (e.g., $Ve(i)$), and then generates and broadcasts an unreal message; 3) it invades a legal vehicle (e.g., $Ve(i)$) to acquire $Sk(i)$, and generates and broadcasts an unreal message in the name of $Ve(i)$; 4) if it is a revoked vehicle (e.g., $Ve(i)$), it leverages its own expired trust certificate to generate and broadcast an unreal message; and 5) it stores an emergency message $Ms(i, \mathcal{E})$ from a legal vehicle (e.g., $Ve(i)$) for a while and rebroadcasts it when $\mathcal{E}$'s status changes.

In fact, however, every emergency message (e.g., $Ms(i, \mathcal{E})$) contains a digital signature (i.e., $Ds_b(i, \mathcal{E})$) and any modification to it can be easily checked out by message receivers, thus an external adversary will not adopt the first strategy. Besides, $Ds_b(i, \mathcal{E})$ is signed through utilizing $Sk(i)$ which is protected in $Ve(i)$'s trusted hardware, thus an external adversary cannot steal $Sk(i)$ and generate a message in the name of $Ve(i)$, even it owns $Tc(i)$, and it will not also adopt the second and third strategies. Furthermore, every trust certificate (e.g., $Tc(i)$) and every emergency message (e.g., $Ms(i, \mathcal{E})$) contain timestamps [i.e., $Ts_C(i)$ and $Ts_b(i, \mathcal{E})$, respectively], thus an expired trust certificate and an emergency message that has been stored and rebroadcasted can be easily checked out by message receivers, thus an external adversary will not adopt the last two strategies.

Thus, the TCEMD model is of strong robustness against BUEM behavior in external attack.

2) RUTF Behavior in External Attack: In our model, an external adversary may adopt the following strategies to carry out RUTF behavior: 1) it manipulates a trust feedback set $TF(j, \mathcal{E})$ of a legal vehicle (e.g., $Ve(j)$) through modifying $Fs(i, j, \mathcal{E})$ according to (13); 2) it invades a legal vehicle (e.g., $Ve(j)$) to obtain $Sk(j)$, and generates and reports unfair trust feedbacks in the name of $Ve(j)$; and 3) it invades $\mathcal{BI}$ and $\mathcal{TF}$ tables to directly modify the trust information in them.

$$Tr_n(i) = \begin{cases} \frac{Wb(i)+Wr(i)}{2} * \frac{\sum_{Tt(i,j,\mathcal{E})\in TT(i)} Fs(i,j,\mathcal{E}) * Tr(j)}{\sum_{Tt(i,j,\mathcal{E})\in TT(i)} Tr(j)}, & \text{if } \sum_{Tt(i,j,\mathcal{E})\in TT(i)} Tr(j) > 0 \\ \lambda * Tr(i), & \text{otherwise} \end{cases} \tag{22}$$

In reality, however, every trust feedback set (e.g., $TF(j, \mathcal{E})$) includes a digital signature (i.e., $Ds_r(j, \mathcal{E})$) and any modification to it can be checked out by CA, so an external adversary will not adopt the first strategy. Besides, $Ds_r(j, \mathcal{E})$ is signed by utilizing $Sk(j)$ which is protected in $Ve(j)$'s trusted hardware, thus an external adversary cannot steal $Sk(j)$ for generating a trust feedback set in the name of $Ve(j)$, and it will not adopt the second strategy. In addition, it is reasonable to assume $\mathcal{BI}$ and $\mathcal{TF}$ tables are primely protected by CA, thus an external adversary cannot effectively invade them and it will not adopt the third strategy.

Thus, the TCEMD model is of strong robustness against RUTF behavior in external attack.

3) BUEM Behavior in Internal Attack: In our model, an internal adversary (e.g., $Ve(i)$) may adopt the following strategies to conduct BUEM behavior: 1) If it is a witness of an event $\mathcal{E}$, it broadcasts $Ms(i, \mathcal{E})$ reporting $\mathcal{E}^-$ (i.e., $Mc(i, \mathcal{E}) = \mathcal{E}^-$) if witnesses $\mathcal{E}^+$, and broadcasts $Ms(i, \mathcal{E})$ reporting $\mathcal{E}^+$ (i.e., $Mc(i, \mathcal{E}) = \mathcal{E}^+$) if witnesses $\mathcal{E}^-$a and b) If it is a follower of $\mathcal{E}$, it broadcasts $Ms(i, \mathcal{E})$ reporting $\mathcal{E}^-$ (i.e., $Mc(i, \mathcal{E}) = \mathcal{E}^-$) if $Dt(i, \mathcal{E}) \geq Tp(i)$, and broadcasts $Ms(i, \mathcal{E})$ reporting $\mathcal{E}^+$ (i.e., $Mc(i, \mathcal{E}) = \mathcal{E}^+$) if $Dt(i, \mathcal{E}) \leq -Tp(i)$.

As we have analyzed earlier, even quite a honest vehicle may also broadcast unreal messages with a certain probability due to the complex road environment and limited perception and processing ability, so in the TCEMD model, a legal vehicle which broadcasts an unreal message will not be revoked at once. As a result, just as other trust models, the TCEMD model is also not of 100% robustness against BUEM behavior in internal attack, but we introduce several strategies into the TCEMD model to significantly enhance its robustness against BUEM behavior in internal attack.

1) The entity-oriented trust values are incorporated into data-oriented trust evaluation in an efficient way, because a vehicle's trust level is able to reflect the quality of its messages to some degree.
2) Every message receiver considers the messages reporting the different statuses of an emergency event together, since they reflect the distinct road conditions at the same spot.
3) Every message receiver considers as many as possible messages from distinct message broadcasters together, since almost every vehicle may broadcast unreal messages due to subjective and objective reasons. These above strategies can obviously improve the robustness of our model against BUEM behavior in internal attack, and the detailed comparisons with some other models are presented in Section VI.

4) RUTF Behavior in Internal Attack: In our model, an internal adversary (e.g., $Ve(j)$) may adopt the following strategies to execute RUTF behavior: 1) it praises itself by reporting a positive trust feedback $Tf(j, j, \mathcal{E})$, where $Fs(j, j, \mathcal{E}) = 1$; 2) it reports a trust feedback about an expired or forged message; 3) it sets $Fs(i, j, \mathcal{E})$'s value beyond $\{0, 1\}$. d) It reports trust feedbacks for a vehicle more than once with respect to the same message; 4) it inflates the trust value of a vehicle that colludes with it (e.g., $Ve(i) \in VC(j)$) by reporting a positive trust feedback $Tf(i, j, \mathcal{E})$, in which $Fs(i, j, \mathcal{E}) = 1$; and 5) it deflates the trust value of a vehicle not colluding with it (e.g., $Ve(i) \notin VC(j)$) by reporting a negative trust feedback $Tf(i, j, \mathcal{E})$, in which $Fs(i, j, \mathcal{E}) = 0$.

In practice, however, every trust feedback (e.g., $Tf(i, j, \mathcal{E})$) is checked whether $i \neq j$ by CA. Besides, $Tf(i, j, \mathcal{E})$ contains the timestamp of when $Ms(i, \mathcal{E})$ is generated (i.e., $Ts_b(i, \mathcal{E})$) and the digital signature signed by leveraging the private key of message broadcaster (i.e., $Ds_b(i, \mathcal{E})$), thus a trust feedback with respect to an expired or forged message can be checked out by CA. Meanwhile, $Fs(i, j, \mathcal{E})$ is checked whether within $\{0, 1\}$ by CA. Moreover, if there exist several trust feedbacks from $Ve(j)$ for $Ve(i)$ with respect to the same message (i.e., with the same values in Id_b, Id_r, Ds_b fields of $\mathcal{TF}$ table), CA only reserves the latest one. As a result, an internal adversary cannot utilize the first four strategies. That is, the TCEMD model is of strong robustness against the first four kinds of strategies of RUTF behavior in internal attack.

However, even quite a honest vehicle may also report unfair trust feedbacks with a certain probability due to the complex road environment and limited perception and processing ability, so in the TCEMD model, a legal vehicle that reports an unfair trust feedback will not be revoked at once. As a result, just like other trust models, the TCEMD model cannot provide 100% robustness against the other two kinds of strategies of RUTF behavior in internal attack, but we incorporate several methods into the TCEMD model to greatly enhance its robustness against them: 1) when updating a vehicle's trust information, every trust feedback reporter (e.g., $Ve(i)$) is checked whether $Ir(i) = \text{FALSE}$, and the trust feedbacks from a revoked vehicle are disregarded by CA. 2) when CA calculating vehicles' trust values, every feedback reporter's trust value (e.g., $Tr(i)$) is adopted as primary weight [as revealed in (22)]. In concrete terms, the trust feedback from a vehicle with low $Tr(i)$ is assigned a small weight, and vice versa. The above methods can significantly enhance the robustness of our model against the other two kinds of strategies of RUTF behavior in internal attack, and the detailed comparisons with some other models are provided in Section VI.

B. Failure Tolerance Analysis

In this part, we analyze the failure tolerance features of our model in terms of the failure of a fraction of RSUs and temporary failure of CA in detail.

It should be noted that CA is not involved in the emergency message dissemination stage of the TCEMD model. In other words, CA is offline in respect to emergency message generation, broadcasting, and trust evaluation. Furthermore, in the TCEMD model, the validity period of each trust certificate is set as Γ', and CA updates vehicles' trust information at the interval of Γ (in which $\Gamma < \Gamma'$). In addition, when a vehicle (e.g., $Ve(i)$) is within the communication range of any available RSU, it can request for new trust certificate (i.e., $Tc(i)$) from CA via the RSU at the interval of Γ, and if it does not receive $Tc(i)$, it tries to request for $Tc(i)$ again at once when it drives into the communication range of another available RSU. Furthermore, Γ' and Γ can be adjusted so as to ensure that the vast majority of vehicles are able to drive from the

communication range of an available RSU into that of another available RSU within a short period of time, that is far smaller than $\Delta\Gamma$ (i.e., $\Gamma' - \Gamma$). Besides, when a vehicle (e.g., $Ve(j)$) drives into the communication range of any available RSU, it can immediately report the trust feedback set (e.g., $TF(j, \mathcal{E})$) stored in its local storage to CA via the RSU, and if it does not receive the corresponding acknowledgment (i.e., $Ac(j, \mathcal{E})$), it tries to report $TF(j, \mathcal{E})$ to CA again once it drives into the communication range of another available RSU. Furthermore, Ψ and Ω can be adjusted so that $Ts_{n'} - Ts_b(i, \mathcal{E}) \leq \Psi$ and $Ts_{n'} - Ts_r(j, \mathcal{E}) \leq \Omega$ almost always hold when there exists no attack or malicious behavior.

As a result, the failure of a fraction of RSUs will not affect the normal running of the TCEMD model, and the temporary failure of CA has no significant negative effect on the emergency message dissemination in the TCEMD model as long as the failure duration of CA is smaller than $\Delta\Gamma$ (i.e., $\Gamma' - \Gamma$).

C. Compatibility Analysis

In this part, we analyze the compatibility of the TCEMD model for three kinds of special situations in detail.

1) Special Situation-I: If a follower (e.g., $Ve(j)$) only accumulates a message about $\mathcal{E}$ (e.g., from $Ve(i)$) when it moves into the neighborhood of $\mathcal{E}$'s location (i.e., $Ds(j, \mathcal{E}) \in (Mw, Md]$), (7) can be reduced to

$$Dt(j, \mathcal{E}) = Mc'(i, \mathcal{E}) \tag{26}$$

and $Ve(j)$ can still derive $Dt(j, \mathcal{E})$ as well as make its decision through the TCEMD model. In this situation, $Dt(j, \mathcal{E})$ is entirely determined by $\mathcal{E}$'s status reported by $Ve(i)$, whether $Ve(i)$ is trustworthy or not. To improve the correct decision probability of $Ve(j)$, (26) can be adjusted to

$$Dt(j, \mathcal{E}) = Mc'(i, \mathcal{E}) * Tr(i) \tag{27}$$

which is similar to the decision strategy in RA model. Accordingly, (7) can be extended to

$$Dt(j, \mathcal{E}) = \begin{cases} \frac{\sum_{Ms(i,\mathcal{E}) \in MS(j,\mathcal{E})} Mc'(i,\mathcal{E}) * Tr(i)}{\sum_{Ms(i,\mathcal{E}) \in MS(j,\mathcal{E})} Tr(i)}, & \text{if } |MS(j, \mathcal{E})| > 1 \\ Mc'(i, \mathcal{E}) * Tr(i), & \text{otherwise} \end{cases} \tag{28}$$

thus the TCEMD model can provide a good compatibility for this special situation.

2) Special Situation-II: If a follower (e.g., $Ve(j)$) is already in the neighborhood of $\mathcal{E}$'s location (i.e., $Ds(j, \mathcal{E}) \in (Mw, Md]$) when it receives the first message about $\mathcal{E}$ (e.g., from $Ve(i)$), $Ve(j)$ can still make an immediate decision based on $Ms(i, \mathcal{E})$ and (28) by leveraging the TCEMD model, so our model has a good compatibility for this special situation.

3) Special Situation-III: In practice, a malicious vehicle (e.g., $Ve(i)$) may broadcast a message reporting a forged emergency event's (e.g., $\tilde{\mathcal{E}}$) existence status (i.e., $\tilde{\mathcal{E}}^+$), instead of the unreal status of a real emergency event (e.g., $\mathcal{E}$), to deceive subsequent vehicles. At the beginning, message receivers (e.g., $Ve(j)$, $Ve(j')$, etc.) make decisions based on $Ve(i)$'s single message (i.e., $Ms(i, \tilde{\mathcal{E}})$) and (28). When $Ve(j)$, $Ve(j')$, etc. move into the neighborhood of $\tilde{\mathcal{E}}$'s location so that $Ds(\bar{j}, \tilde{\mathcal{E}}) \in [0, Mw]$ (where $\bar{j}$ indicates j, j', etc., the same below), they can perceive $\tilde{\mathcal{E}}$'s actual status (i.e., $As(\bar{j}, \tilde{\mathcal{E}}) = \tilde{\mathcal{E}}^-$) which is not consistent with that reported previously by $Ve(i)$. For each $\bar{j} \in \{j, j', \ldots\}$, if $Ve(\bar{j})$ is honest, it reports a negative trust feedback for $Ve(i)$ to CA, and broadcasts $Ms(\bar{j}, \tilde{\mathcal{E}})$ reporting $\tilde{\mathcal{E}}^-$ to subsequent vehicles (if it has not done so before); otherwise, it reports an active trust feedback for $Ve(i)$ to CA, and broadcasts $Ms(\bar{j}, \tilde{\mathcal{E}})$ reporting $\tilde{\mathcal{E}}^+$ to subsequent vehicles (if it has not done so before). Thus, subsequent message receivers (e.g., $Ve(k)$) can make decisions based on several messages about $\tilde{\mathcal{E}}$ (e.g., $Ms(j, \tilde{\mathcal{E}})$, $Ms(j', \tilde{\mathcal{E}})$, etc.) and (28). Consequently, the TCEMD model is of a good compatibility for this special situation.

D. Incentive Mechanism Analysis

As we know, incentive mechanisms are crucial to every trust model in VANETs (including the TCEMD model), since they can inspire vehicles to actively and honestly participate in the emergency message dissemination.

In this article, we notice the fact that the emergency messages in VANETs can be disseminated among vehicles in a cascading way. That is, a vehicle's message can influence the decisions of its several subsequent vehicles and not limit to its successors. Besides, we model the source of influence power as the entity-oriented trust values. In order to improve the influence power, every vehicle (e.g., $Ve(i)$) should try its utmost to improve its trust value (i.e., $Tr(i)$). As shown in (22), to improve $Tr_n(i)$, $\forall Ve(i) \in VN$ should try its best to broadcast as many emergency messages as possible and report as many trust feedbacks as possible to raise $Nb(i)$ and $Nr(i)$, and then increase $Wb(i)$ and $Wr(i)$, respectively, as well as broadcast real emergency messages to raise $Fs(i, j, \mathcal{E})$. If a vehicle (e.g., $Ve(i)$) refuses to broadcast emergency messages or report trust feedbacks, or broadcasts unreal messages, $Tr(i)$ will continually decrease to (or keep nearly unchanged as) a low value, and if low value, and if $Nn(i) > \Theta$ and $Tr(i) < Tp(C)$, $Ve(i)$ will be revoked from the VANET system by CA. Therefore, the vehicles in the TCEMD model are well-motivated to actively and honestly take part in the emergency.

In addition, as CA maintains the trust information of all the vehicles in $\mathcal{BI}$ and $\mathcal{TF}$ tables, it is easy to incorporate several rewards (e.g., ranking points, prize money, etc.) into our model. Besides, a vehicle's trust value in our model can be combined with the point on the driver's license, as they can be managed by the same CA (e.g., TSA) and both they aim at motivating honest behaviors and punishing malicious behaviors in roads (The detailed analysis is omitted here due to the limited space).

VI. Performance Evaluation

In this section, we first utilize the famous SUMO simulator to deploy a typical highway environment, and then evaluate the performance of the TCEMD model by varying the percentage of malicious vehicles and compared with some excellent models.

TABLE I
SETTINGS OF SIMULATION ENVIRONMENT

Descriptions	Values
Length of simplified highway	8000 m
Number of vehicles on the simplified highway	200
Number of lanes on the simplified highway	3
Average driving speed of vehicle on the fast lane	32 m/s*
Average driving speed of vehicle on the middle lane	28 m/s*
Average driving speed of vehicle on the slow lane	21 m/s*
Average spacing between vehicles on the fast lane	150 m*
Average spacing between vehicles on the middle lane	110 m*
Average spacing between vehicles on the slow lane	75 m*
Spacing between RSUs on the simplified highway	300 m
Maximum single-hop communication distance	300 m

* The average driving speed of vehicle and the average spacing between vehicles here are set based on the provisions of the road traffic safety law in China.

TABLE II
SETTINGS OF PARAMETERS IN THE TCEMD MODEL

Parameters	Values	Parameters	Values
Mw	100 m	Γ	300 s*
Md	300 m	Γ'	350 s*
Mi	600 m	Φ	1 s*
$Tp(C)$	0.05	Ψ	70 s*
Θ	50	Ω	5 h*
λ	0.95		

* In the simulations, Γ, Γ', Φ, Ψ, and Ω are set as relatively low values to make the effect of TCEMD model more visible.

A. Simulation Settings

In this part, we first study the real road network information of Guangzhou beltway (which is a typical highway with three lanes per direction) by utilizing the famous OSM[3] tool. Based on this, we deploy a simplified one-way highway environment with three lanes (i.e., fast lane, middle lane, and slow lane) by leveraging the well-known SUMO simulator. A small fragment of simulation environment is shown in Fig. 7. The justifications for adopting a typical highway as the simulation environment are summed up as follows: 1) the traffic accidents on a highway generally lead to serious consequences (e.g., multi-injuries with numerous mortal wounds and a high mortality rate, and the impact is likely to spread to the entire road network), so the trustworthy emergency message dissemination on the highway is of great importance for the purpose of improving road safety and traffic efficiency and 2) it is convenient to deploy our model and some excellent models in the highway simulation environment, as well as comprehensively compare their performance by varying the percentage of malicious vehicles and repeating tests enough times for each case.

The specific settings of the simulation environment and parameters in the TCEMD model are illustrated in Table I and Table II, respectively, and $Tp(i)$ is generated by randomly sampling the real numbers within the range of [0, 1], following the normal distribution $N(\mu, \sigma^2)$ as:

$$f(x|\mu,\sigma) = \frac{1}{\sqrt{2\pi}\sigma} * \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) \tag{29}$$

where the values of both expected value (i.e., μ) and standard deviation (i.e., σ) are set as 0.5. Furthermore, the percentages of high-, medium-, low-authority-level vehicles are assumed to be 5%, 10%, and 85%, respectively, and every vehicle's initial trust value is set based on its authority level as revealed in (2). Besides, we assume that every vehicle (e.g., $Ve(i)$) of which $Ds(i, \mathcal{E}) \in [0, Mw]$ fails to precisely perceive the actual status of an emergency event (e.g., $\mathcal{E}$) with a probability of 5% due to the complex road environment as well as limited perception and processing ability.

Moreover, we present the following five aspects to comprehensively evaluate the performance of the TCEMD model through comparison with several excellent models.

1) *Th:* Average trust value of honest vehicles.
2) *Tm:* Average trust value of malicious vehicles.
3) *Pc:* Correct decision percentage of vehicles.
4) *Nt:* Number of broadcasting emergency messages in terms of an emergency event.
5) *Nu:* Number of broadcasting unreal emergency messages in terms of an emergency event.

As mentioned earlier, the primary purpose of incorporating trust models into VANETs is to improve road safety and traffic efficiency, thus among the above aspects, *Pc* is the most important one. Besides, *Th* and *Tm* intuitively reveal the trust value variations of honest and malicious vehicles, respectively. Meanwhile, *Nt* indicates the cost of broadcasting emergency messages (as well as the ability of a trust model to reduce the total number of emergency messages and relieve the wireless channel collision problem in the VANET system), and *Nu* reveals the ability of a trust model to limit the dissemination of unreal messages. Intuitively, in a VANET system containing a certain percentage of malicious vehicles, a trust model with higher *Pc*, lower *Nt*, and lower *Nu* can be considered to have stronger robustness, and vice versa.

Furthermore, since we have proved that the TCEMD model has strong robustness against both BUEM and RUTF behaviors in external attack and the first four strategies of RUTF behavior in internal attack, good failure tolerance features and compatibility for several kinds of special situations, as well as effective incentive mechanisms through detailed theoretical analysis in Section V, here we mainly focus on evaluating the robustness of our model (i.e., specific degree of resistance) against BUEM behavior and the last two strategies of RUTF behavior in internal attack.

In concrete terms, malicious vehicles in internal attack may try their utmost to: 1) broadcast unreal emergency messages to deceive subsequent vehicles (i.e., take BUEM behavior); and 2) report unfair trust feedbacks to CA for inflating/deflating other vehicles' trust values and taking BUEM behavior for a longer time before being revoked from the VANET system (i.e., take both BUEM behavior and the last two strategies of RUTF behavior). For ease of illustration, we name the above

[3]OpenStreetMap: https://www.openstreetmap.org

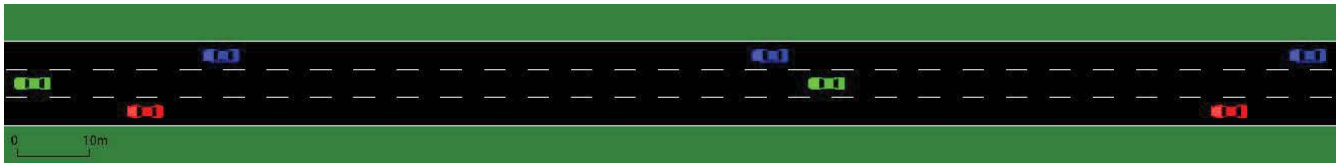


Fig. 7. Small fragment of simulation environment.

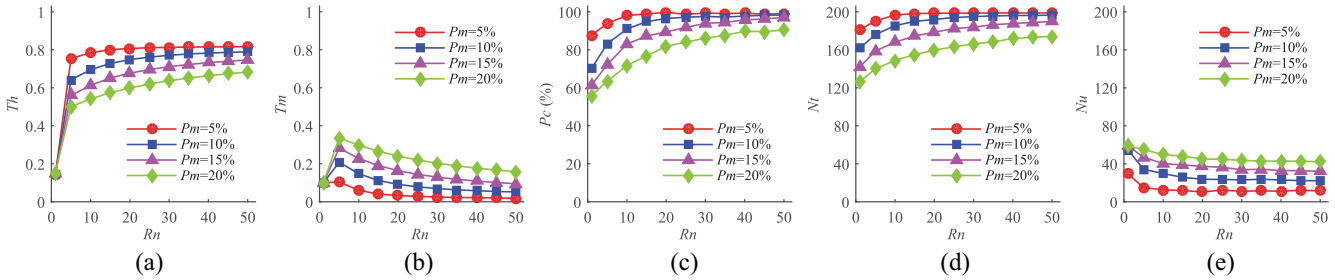


Fig. 8. Variation curves of several aspects in the TCEMD model versus *Rn* in *Case-I*. (a) *Th*. (b) *Tm*. (c) *Pc*. (d) *Nt*. (e) *Nu*.

two cases as *Case-I* and *Case-II*, and verify the robustness of our model and compare it with several excellent models in the two cases, respectively.

B. Robustness Verification in Case-I

In this part, we mainly validate the robustness of our model in *Case-I*, where malicious vehicles are assumed to only take BUEM behavior, i.e., try their utmost to broadcast unreal emergency messages for deceiving subsequent vehicles, but report fair trust feedbacks to CA. Specifically, we vary the percentage of malicious vehicles (denoted as *Pm*) from 5% to 20%, and for each *Pm*, we first initialize our model and then implement the operations in the other stages of our model for 50 rounds. The round number's (marked as *Rn*) value is within [1, 50], and the duration of each round is equal to Γ (i.e., 300 s). That is, after each round, CA updates vehicles' trust information in $\mathcal{BI}$ table and vehicles request for their new trust certificates. The above procedures are repeated 1000 times for each *Pm*, and the average results are illustrated in Fig. 8.

From Fig. 8(a), we can discover that the average trust value of honest vehicles (i.e., *Th*) in each case first rapidly increases when $Rn \in [1, 5)$ and then slowly raises or basically remains unchanged (as a relatively high value) when $Rn \in [5, 50]$. In addition, with the raise of *Pm* from 5% to 20%, *Th* slightly decreases.

Fig. 8(b) illustrates that the average trust value of malicious vehicles (i.e., *Tm*) in each case first grows to a certain degree when $Rn \in [1, 5)$ (as our model cannot efficiently distinguish between honest and malicious vehicles in the very beginning) and then gradually decreases or basically keeps consistent (as a relatively low value) when $Rn \in [5, 50]$. Moreover, with the increase of *Pm* from 5% to 20%, *Tm* slightly raises.

From Fig. 8(c), we can easily find that the correct decision percentage of vehicles (i.e., *Pc*) in each case first quickly increases and then remains nearly unchanged (as a relatively high value). Moreover, with the raise of *Pm* from 5% to 20%, *Pc* slightly decreases.

Fig. 8(d) shows that the number of broadcasting emergency messages in terms of an emergency event (i.e., *Nt*) first gradually raises and then keeps nearly constant (as a relatively low value which is smaller than the total number of vehicles, i.e., 200). This is because in the beginning the trust values of the majority of vehicles are so low that it is difficult for the events reported by them to be trusted and broadcasted by message receivers, and with the growth of *Th* and decrease of *Tm*, an increasing number of events reported by honest vehicles can be trusted and broadcasted by message receivers. Meanwhile, with the raise of *Pm* from 5% to 20%, *Nt* slightly decreases.

From Fig. 8(e), we can discover that the number of broadcasting unreal emergency messages in terms of an emergency event (i.e., *Nu*) in each case first decreases and then basically keeps constant (as a relatively low value). This mainly benefits from the strategies in the TCEMD model (i.e., every follower only broadcasts its own message if it is quite sure about an event's status). Moreover, with the raise of *Pm* from 5% to 20%, *Nu* slightly increases.

C. Robustness Comparisons in Case-I

In this part, we compare the robustness of the TCEMD model and several outstanding models, including MV [31], CIO [35], and RA [26] models, in *Case-I* (the comparison with LT [36] model is omitted here as this model does not define the source of influence power). Specifically, we first deploy MV, CIO, and RA models in our simulation environment with few necessary modifications. In these models, malicious vehicles are also assumed to merely conduct BUEM behavior, and every witness takes the same strategy with that in the TCEMD model. However, the strategy of every follower in these models is quite different from that in TCEMD models.

1) In MV model, every follower makes a decision based on the messages reporting $\mathcal{E}^+/\mathcal{E}^-$ from its precursors: If the number of reporting $\mathcal{E}^+$ is not less than that of reporting $\mathcal{E}^-$, it trusts $\mathcal{E}^+$ and reports $\mathcal{E}^+$ (if it is honest)/$\mathcal{E}^-$ (otherwise) to subsequent vehicles; otherwise, it trusts

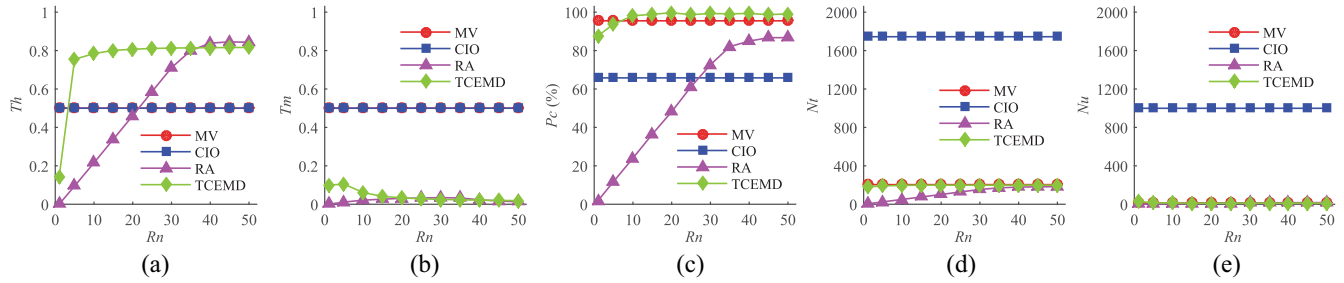


Fig. 9. Variation curve comparisons of several aspects in MV, CIO, RA, and TCEMD models versus *Rn* in *Case-I* when $Pm = 5\%$. (a) *Th*. (b) *Tm*. (c) *Pc*. (d) *Nt*. (e) *Nu*.

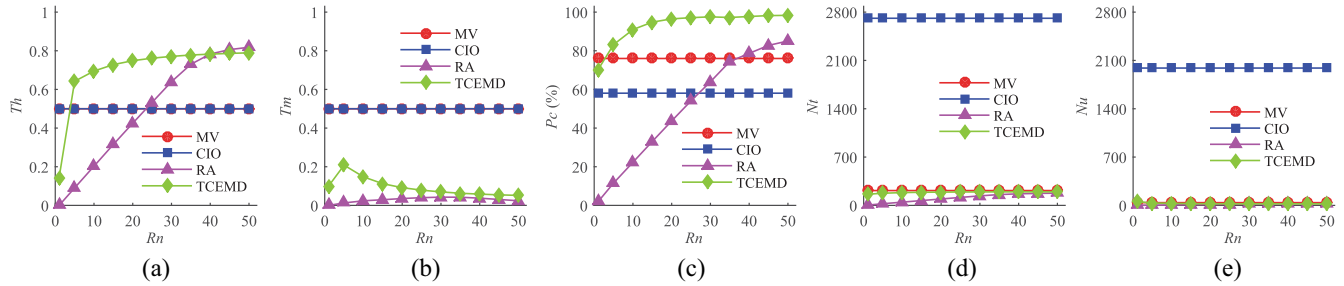


Fig. 10. Variation curve comparisons of several aspects in MV, CIO, RA, and TCEMD models versus *Rn* in *Case-I* when $Pm = 10\%$. (a) *Th*. (b) *Tm*. (c) *Pc*. (d) *Nt*. (e) *Nu*.

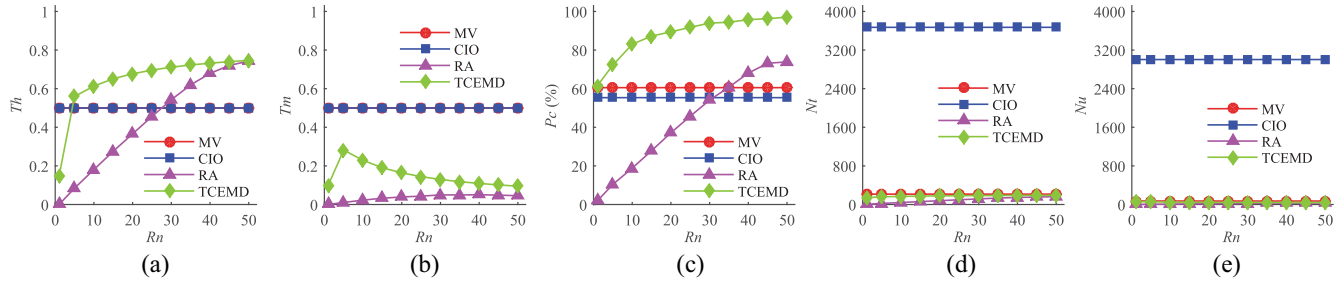


Fig. 11. Variation curve comparisons of several aspects in MV, CIO, RA, and TCEMD models versus *Rn* in *Case-I* when $Pm = 15\%$. (a) *Th*. (b) *Tm*. (c) *Pc*. (d) *Nt*. (e) *Nu*.

$\mathcal{E}^-$ and reports $\mathcal{E}^-$ (if it is honest)/$\mathcal{E}^+$ (otherwise) to subsequent vehicles. In addition, a malicious follower can relay part of precursors' messages that report the same status of $\mathcal{E}$ as reported by itself, and the subsequent vehicles cannot effectively distinguish between the messages relayed by its precursors and those generated by its precursors in our simulation environment.

2) In CIO model, every follower only relays witnesses' messages reporting $\mathcal{E}^+/\mathcal{E}^-$ without broadcasting its own message to subsequent vehicles, and makes a decision based on witnesses' messages (Huang *et al.* [35] showed that CIO model achieves its best performance when only witnesses' messages are considered): if the number of reporting $\mathcal{E}^+$ is not less than that of reporting $\mathcal{E}^-$, it trusts $\mathcal{E}^+$; otherwise, it trusts $\mathcal{E}^-$. Besides, a malicious follower can disguise itself as a witness and report a false status of a certain event (if it trusts $\mathcal{E}^+$, it reports $\mathcal{E}^-$; otherwise, it reports $\mathcal{E}^+$), and the subsequent vehicles cannot effectively distinguish it from actual witnesses in our simulation environment.

3) In RA model, every follower makes a decision based on a single message about an emergency event. It is reasonable to assume that vehicles cannot change their decisions frequently, therefore we assume that every follower makes a decision based on the first message (it receives) reporting $\mathcal{E}^+/\mathcal{E}^-$. Besides, the original RA model does not consider the message dissemination among multihop vehicles, so we extend this model by introducing the strategy for each follower: if it trusts $\mathcal{E}^+$, it reports $\mathcal{E}^+$ (if it is honest)/$\mathcal{E}^-$ (otherwise) to subsequent vehicles, and if it trusts $\mathcal{E}^-$, it reports $\mathcal{E}^-$ (if it is honest)/$\mathcal{E}^+$ (otherwise) to subsequent vehicles.

Afterward, we vary *Pm* from 5% to 20% and test the performance of MV, CIO, and RA models for each *Pm* (just like we does in Section VI-B), respectively. The average comparative results among MV, CIO, RA, and TCEMD models for each *Pm* are revealed in Figs. 9–12, respectively. In addition, as there is no consideration of vehicles' trust values in MV and CIO models, we assume that both *Th* and *Tm* in the two models keep constant as 0.5 to make the comparison results more intuitive.

Figs. 9(a)–12(a) indicate that *Th* in the TCEMD model is significantly higher than that in the other three models for the majority of *Rn* and *Pm*, and Figs. 9(b)–12(b) shows that *Tm* in

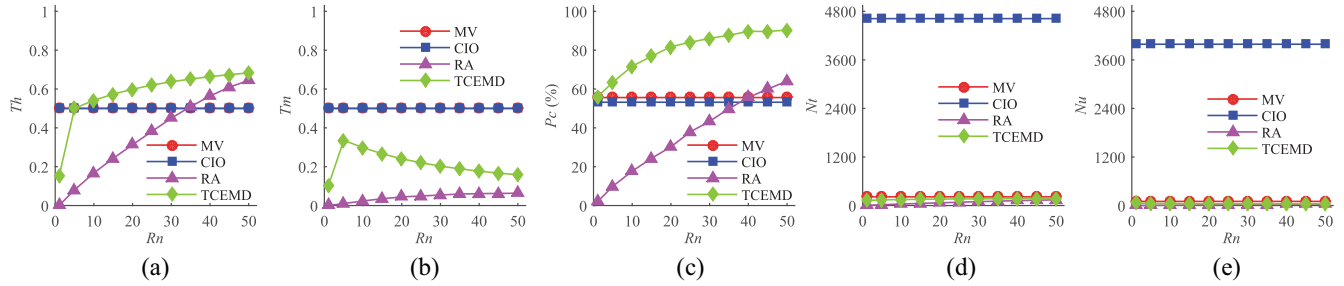


Fig. 12. Variation curve comparisons of several aspects in MV, CIO, RA, and TCEMD models versus *Rn* in *Case-I* when $Pm = 20\%$. (a) *Th*. (b) *Tm*. (c) *Pc*. (d) *Nt*. (e) *Nu*.

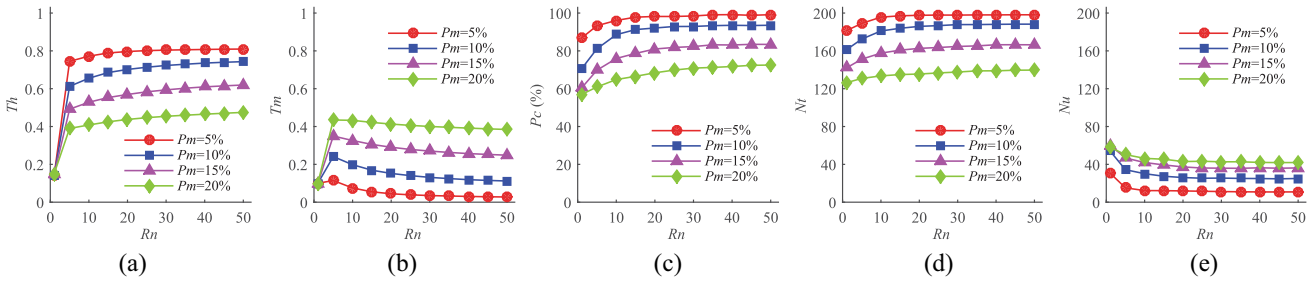


Fig. 13. Variation curves of several aspects in the TCEMD model versus *Rn* in *Case-II*. (a) *Th*. (b) *Tm*. (c) *Pc*. (d) *Nt*. (e) *Nu*.

the TCEMD model is higher than that in RA model to some degree for the majority of *Rn* and *Pm*, and is obviously lower than that in MV and CIO models for each *Rn* and *Pm*.

From Figs. 9(c)–12(c), we can easily find that *Pc* in MV and CIO models for each *Pm* remains constant, as there is no trust feedback mechanism in these two models. Besides, *Pc* in the TCEMD model for each *Pm* first quickly raises and then remains nearly unchanged as a relatively high value, while *Pc* in RA model for each *Pm* first slowly increases and then keeps basically unchanged as a relatively low value much lower than that in the TCEMD model. Furthermore, *Pc* in the TCEMD model is higher than that in the other models for the majority of *Rn* and *Pm*, and the advantage becomes increasingly obvious with the raise of *Pm* from 5% to 20%.

Figs. 9(d)–12(d) show that *Nt* in MV and CIO models for each *Pm* keeps constant, since there is no trust feedback mechanism in these two models. In addition, *Nt* in the TCEMD model is lower than that in MV model and higher than that in RA model to a small degree for the majority of *Rn* and *Pm*, and *Nt* in CIO model is significantly higher than that in the other models for each *Rn* and *Pm*, as every follower in CIO model may relay multiple emergency messages.

From Figs. 9(e)–12(e), we can discover that the comparative variation curves of *Nu* among four kinds of models for each *Pm* are similar to those of *Nt*, respectively.

Through the above analysis, we can easily find that the TCEMD model has obviously higher *Pc* and relatively lower *Nt* and *Nu* for the majority of *Pm* and *Rn* when compared with the other models in *Case-I*, so the TCEMD model has stronger robustness against BUEM behavior in internal attack than the other models.

D. Robustness Verification in Case-II

In this part, we mainly validate the robustness of our model in *Case-II*, where malicious vehicles are assumed to take both BUEM behavior and the last two strategies of RUTF behavior, i.e., try their utmost to report unfair trust feedbacks to CA for inflating/deflating other vehicles' trust values and broadcasting unreal emergency messages for a longer time before being revoked from the VANET system. To maximize the destructive power of internal attack, we assume that all the malicious vehicles collude with each other. In other words, each malicious vehicle reports positive trust feedbacks for malicious message broadcasters to inflate their trust values, and reports negative trust feedbacks for honest message broadcasters to deflate their trust values. The specifical experimental method is in line with that in Section VI-B, and the average results are illustrated in Fig. 13.

From Fig. 13, we can easily find that the variation rules of *Th*, *Tm*, *Pc*, *Nt*, and *Nu* in *Case-II* are basically consistent with those in *Case-I* as shown in Fig. 8, respectively. Furthermore, with the growth of *Pm* from 5% to 20%, the descending speed of *Th*, *Pc*, *Nt* and the ascending speed of *Tm*, *Nu* in *Case-II* are relatively higher than those in *Case-I*, respectively. This is because the destructive power of malicious vehicles in *Case-II* is larger than that in *Case-I*.

E. Robustness Comparisons in Case-II

In this part, we compare the robustness of the TCEMD model and several outstanding models in *Case-II*. Specifically, in MV, CIO, and RA models, malicious vehicles are also assumed to take both BUEM behavior and the last two strategies of RUTF behavior: 1) in terms of BUEM behavior, vehicles' strategies in MV, CIO, and RA models are in line with those in *Case-I* (as revealed in Section VI-C), respectively and 1) in terms of the last two strategies of RUTF behavior, vehicles' strategies in MV, CIO, and RA models are in line with those in the TCEMD model in *Case-II* (as shown in Section VI-D). The specific experimental method is in keeping

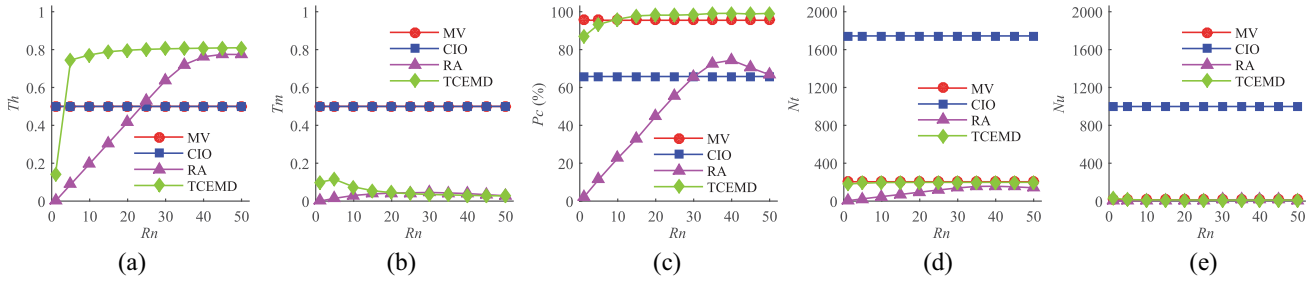


Fig. 14. Variation curve comparisons of several aspects in MV, CIO, RA, and TCEMD models versus *Rn* in *Case-II* when $Pm = 5\%$. (a) *Th*. (b) *Tm*. (c) *Pc*. (d) *Nt*. (e) *Nu*.

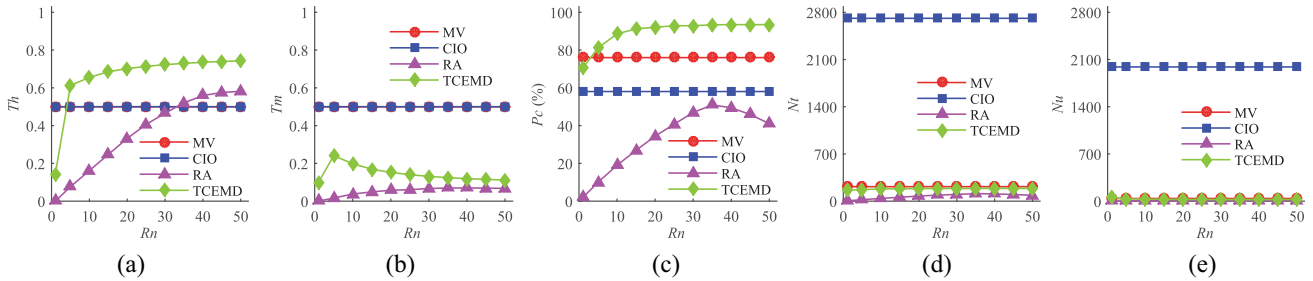


Fig. 15. Variation curve comparisons of several aspects in MV, CIO, RA, and TCEMD models versus *Rn* in *Case-II* when $Pm = 10\%$. (a) *Th*. (b) *Tm*. (c) *Pc*. (d) *Nt*. (e) *Nu*.

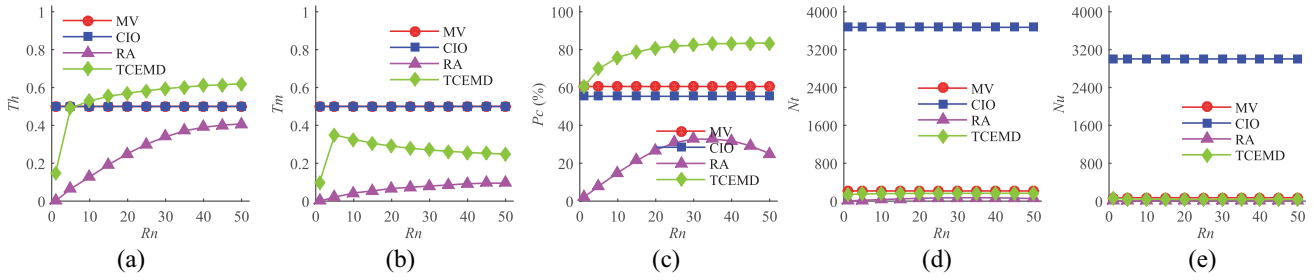


Fig. 16. Variation curve comparisons of several aspects in MV, CIO, RA, and TCEMD models versus *Rn* in *Case-II* when $Pm = 15\%$. (a) *Th*. (b) *Tm*. (c) *Pc*. (d) *Nt*. (e) *Nu*.

with that in Section VI-B, and the average comparative results among four models for each *Pm* are shown in Figs. 14–17, respectively. Besides, we also assume that both *Th* and *Tm* in MV and CIO models remain unchanged as 0.5 to make the comparison results more intuitive.

Figs. 14(a)–17(a) reveal that the variation rule of *Th* in each model is similar to that in *Case-I* [as shown in Figs. 9(a)–12(a)], respectively. Meanwhile, Figs. 14(b)–17(b) indicate that the variation rule of *Tm* in each model is basically consistent with that in *Case-I* [as shown in Figs. 9(b)–12(b)], respectively. Moreover, with the growth of *Pm* from 5% to 20%, both the descending speed of *Th* and the ascending speed of *Tm* in RA and TCEMD models in *Case-II* are relatively higher than those in *Case-I*, respectively.

From Figs. 14(c)–17(c), we can easily discover that *Pc* in MV and CIO models for each *Pm* still remains unchanged. Besides, *Pc* in the TCEMD model for each *Pm* first quickly raises and then remains nearly unchanged as a relatively high value, while *Pc* in RA model for each *Pm* first slowly increases and then decreases to a relatively low value much lower than that in the TCEMD model. In addition, with the increase of *Pm* from 5% to 20%, the descending speed of *Pc* in RA and TCEMD models in *Case-II* is relatively higher than that in *Case-I*, respectively. Moreover, *Pc* in the TCEMD model is higher than that in the other models for the majority of *Rn* and *Pm*, and the advantage is obvious when $Rn \geq 5$ and $Pm \geq 10\%$.

Figs. 14(d)–17(d) and Figs. 14(e)–17(e) indicate that the variation curves of *Nt* and *Nu* in four kinds of models for each *Pm* are similar to those in *Case-I* as revealed in Figs. 9(d)–12(d) and Figs. 9(e)–12(e), respectively.

The above analysis reveals that the TCEMD model has obviously higher *Pc* and relatively lower *Nt* and *Nu* for the majority of *Pm* and *Rn* when compared with the other models in *Case-II*, thus the TCEMD model has stronger robustness against BUEM behavior and the last two strategies of RUTF behavior in internal attack than the other models.

F. Comprehensive Robustness Comparisons

As without adopting digital signature and cryptography technologies, both MV and CIO models cannot effectively resist against BUEM and RUTF behaviors in external attack,

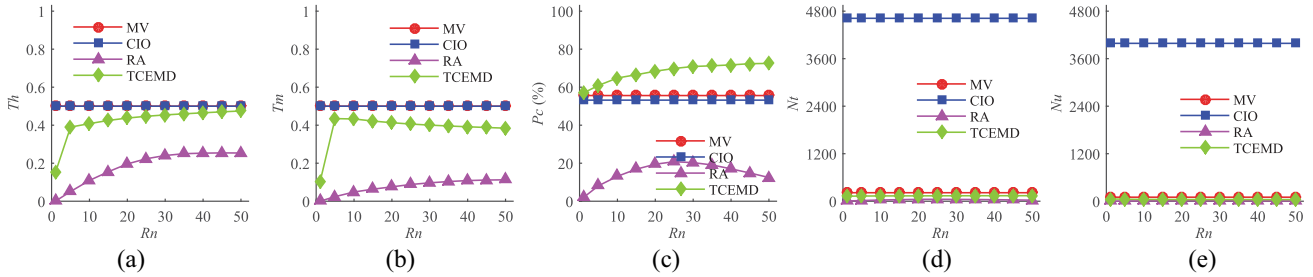


Fig. 17. Variation curve comparisons of several aspects in MV, CIO, RA, and TCEMD models versus *Rn* in *Case-II* when $Pm = 20\%$. (a) *Th*. (b) *Tm*. (c) *Pc*. (d) *Nt*. (e) *Nu*.

TABLE III
COMPREHENSIVE ROBUSTNESS COMPARISON RESULTS AMONG MV, CIO, RA, AND TCEMD MODELS

Attacks and malicious behaviors	MV [31]	CIO [35]	RA [26]	TCEMD
BUEM & RUTF in external attack	None	None	Strong	Strong
BUEM & RUTF in internal attack	TCEMD $\gg$ MV, CIO, RA*			

* "TCEMD $\gg$ MV, CIO, RA" denotes that TCEMD model has significantly stronger robustness than MV, CIO, and RA models.

while both RA and TCEMD models can provide strong robustness against BUEM and RUTF behaviors in external attack, which is proved by the detailed theoretical analysis in [26] and Section V-A. Besides, from the theoretical/simulational results of Section V-A, VI-C, and VI-E, we can derive that the TCEMD model is of significantly stronger robustness against BUEM and RUTF behaviors in internal attack than MV, CIO, and RA models. Consequently, the comprehensive robustness comparison results among the four trust models are indicated in Table III.

VII. CONCLUSION

In this article, we have detailed the proposal of trust cascading in VANETs and presented a novel TCEMD model which incorporates the entity-oriented trust values into data-oriented trust evaluation in an efficient manner. In the proposed model, when an emergency event occurs, the emergency messages can be disseminated among the nearby vehicles in a trust cascading manner, where the entity-oriented trust values (which are evaluated and updated by leveraging the trust certificates and are contained in the messages) are adopted as important weights. Besides, we have detailed the theoretical analysis for the robustness against attacks and malicious behaviors, failure tolerance features, compatibility for special situations, and incentive mechanisms in the TCEMD model. Moreover, we have deployed a typical highway environment by utilizing the famous SUMO simulator and conducted comprehensive simulations and analysis. We have not only evaluated the performance of the TCEMD model but also compared it with MV, CIO, and RA models. The results reveal that the proposed model greatly outperforms the existing models in several cases.

In future work, we will focus on the following two aspects.

1) Comprehensively considering objective trust and subjective trust, then modeling objective trust based on vehicles' capabilities of perception, processing, etc., and modeling subjective trust based on other vehicles' feedback scores on several trust aspects, such as messages' accuracy and timeliness, vehicles' participation degree, and so on.
2) Establishing a multiple factors-based cascading model for emergency messages dissemination in VANETs. As mentioned earlier, a vehicle's message can influence the decisions of its several subsequent vehicles and not limit to its successors (i.e., in a cascading manner), and we consider that the source of influence power can be correspondingly modeled as the combination of multiple factors, including vehicles' objective and subjective trust values, messages' time decay weights, and so on.

REFERENCES

[1] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2377–2396, 4th Quart., 2015.
[2] C. Chen, L. Liu, T. Qiu, Z. Ren, J. Hu, and F. Ti, "Driver's intention identification and risk evaluation at intersections in the Internet of Vehicles," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1575–1587, Jun. 2018.
[3] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 127–139, Mar. 2012.
[4] D. Tian *et al.*, "A distributed position-based protocol for emergency messages broadcasting in vehicular ad hoc networks," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1218–1227, Apr. 2018.
[5] S. Ucar, S. C. Ergen, and O. Ozkasap, "Multihop-cluster-based IEEE 802.11p and LTE hybrid architecture for VANET safety message dissemination," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2621–2636, Apr. 2016.
[6] B. Kloiber, J. Härri, T. Strang, S. Sand, and C. R. Garcia, "Random transmit power control for DSRC and its application to cooperative safety," *IEEE Trans. Depend. Secure Comput.*, vol. 13, no. 1, pp. 18–31, Jan. 2016.
[7] M. Saini, A. Alelaiwi, and A. E. Saddik, "How close are we to realizing a pragmatic VANET solution? A meta-survey," *ACM Comput. Surveys*, vol. 48, no. 2, p. 29, Nov. 2015.
[8] J. Sahoo, E. H.-K. Wu, P. K. Sahu, and M. Gerla, "Binary-partition-assisted MAC-layer broadcast for emergency message dissemination in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 757–770, Sep. 2011.
[9] F. F. Hassanzadeh and S. Valaee, "Reliable broadcast of safety messages in vehicular ad hoc networks," in *Proc. 28th INFOCOM*, 2009, pp. 226–234.
[10] F. Lyu *et al.*, "SS-MAC: A novel time slot-sharing MAC for safety messages broadcasting in VANETs," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3586–3597, Apr. 2018.

[11] K. A. Hafeez, L. Zhao, Z. Liao, and B. N. W. Ma, "A new broadcast protocol for vehicular ad hoc networks safety applications," in *Proc. GLOBECOM*, 2010, pp. 1–5.
[12] H. Yoo and D. Kim, "ROFF: Robust and fast forwarding in vehicular ad-hoc networks," *IEEE Trans. Mobile Comput.*, vol. 14, no. 7, pp. 1490–1502, Jul. 2015.
[13] W. Viriyasitavat, F. Bai, and O. K. Tonguz, "UV-CAST: An urban vehicular broadcast protocol," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 116–124, Nov. 2011.
[14] R. Chen, W.-L. Jin, and A. Regan, "Broadcasting safety information in vehicular networks: Issues and approaches," *IEEE Netw.*, vol. 24, no. 1, pp. 20–25, Jan./Feb. 2010.
[15] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.
[16] J. Li, H. Lu, and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 938–948, Apr. 2015.
[17] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 516–526, Mar. 2017.
[18] S. Tangade, S. S. Manvi, and P. Lorenz, "Decentralized and scalable privacy-preserving authentication scheme in VANETs," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8647–8655, Sep. 2018.
[19] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "VSPN: VANET-based secure and privacy-preserving navigation," *IEEE Trans. Comput.*, vol. 63, no. 2, pp. 510–524, Feb. 2014.
[20] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1711–1720, Mar. 2016.
[21] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 8, pp. 2193–2204, Aug. 2016.
[22] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, "A trust modeling framework for message propagation and evaluation in VANETs," in *Proc. 2nd ITCS*, 2010, pp. 1–8.
[23] Z. Liu, J. Ma, Z. Jiang, H. Zhu, and Y. Miao, "LSOT: A lightweight self-organized trust model in VANETs," *Mobile Inf. Syst.*, vol. 2016, pp. 1–15, Nov. 2016. [Online]. Available: https://www.researchgate.net/publication/311620237_LSOT_A_lightweight_selforganized_trust_model_in_VANETs/citation/download
[24] D. Wang, T. Muller, Y. Liu, and J. Zhang, "Towards robust and effective trust management for security: A survey," in *Proc. 13th TrustCom*, 2014, pp. 511–518.
[25] J. Zhang, "A survey on trust management for VANETs," in *Proc. AINA*, 2011, pp. 105–112.
[26] Q. Li, A. Malip, K. M. Martin, S.-L. Ng, and J. Zhang, "A reputation-based announcement scheme for VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 9, pp. 4095–4108, Nov. 2012.
[27] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1786–1797, Feb. 2017.
[28] R. G. Machado and K. Venkatasubramanian, "Short paper: Establishing trust in a vehicular network," in *Proc. VNC*, 2013, pp. 194–197.
[29] Z. Liu, "Research on key issues for trust modeling in mobile distributed environments," Ph.D. dissertation, School Comput. Sci. Technol., Xidian Univ., Xi'an, China, 2017.
[30] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. 27th INFOCOM*, 2008, pp. 1912–1920.
[31] B. Ostermaier, F. Dotzer, and M. Strassberger, "Enhancing the security of local dangerwarnings in VANETs—A simulative analysis of voting schemes," in *Proc. 2nd ARES*, 2007, pp. 422–431.
[32] H. O. A. Falasi, M. M. Masud, and N. Mohamed, "Trusting the same: Using similarity to establish trust among vehicles," in *Proc. CTS*, 2015, pp. 64–69.
[33] U. F. Minhas, J. Zhang, T. 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 Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 41, no. 3, pp. 407–420, May 2011.
[34] X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Netw.*, vol. 55, no. 1, pp. 107–118, Feb. 2017.
[35] Z. Huang, S. Ruj, M. A. Cavenaghi, M. Stojmenovic, and A. Nayak, "A social network approach to trust management in VANETs," *Peer-to-Peer Netw. Appl.*, vol. 7, no. 3, pp. 229–242, Sep. 2014.
[36] D. Kempe, J. Kleinberg, and É. Tardos, "Maximizing the spread of influence through a social network," in *Proc. 9th SIGKDD*, 2003, pp. 137–146.
[37] K. Rostamzadeh, H. Nicanfar, N. Torabi, S. Gopalakrishnan, and V. C. M. Leung, "A context-aware trust-based information dissemination framework for vehicular networks," *IEEE Internet Things J.*, vol. 2, no. 2, pp. 121–132, Apr. 2015.
[38] 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 Trans. Mobile Comput.*, vol. 14, no. 10, pp. 2101–2115, Oct. 2015.
[39] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1228–1237, May 2015.
[40] M. Jia, H. Wang, B. Ye, and Y. Wang, "A dynamic grouping-based trust model for mobile P2P networks," in *Proc. SCC*, 2016, pp. 848–851.
[41] D. Wu, S. Si, S. Wu, and R. Wang, "Dynamic trust relationships aware data privacy protection in mobile crowd-sensing," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2958–2970, Aug. 2018.
[42] Z. Liu, J. Ma, Z. Jiang, and Y. Miao, "FCT: A fully-distributed context-aware trust model for location based service recommendation," *Sci. China Inf. Sci.*, vol. 60, no. 8, pp. 1–16, Aug. 2017.
[43] X. Li, J. Liu, X. Li, and W. Sun, "RGTE: A reputation-based global trust establishment in VANETs," in *Proc. 5th INCoS*, 2013, pp. 210–214.
[44] W. Bamberger, J. Schlittenlacher, and K. Diepold, "A trust model for intervehicular communication based on belief theory," in *Proc. 2nd SocialCom*, 2010, pp. 73–80.
[45] P. Wex, J. Breuer, A. Held, T. Leinmuller, and L. Delgrossi, "Trust issues for vehicular ad hoc networks," in *Proc. VNC*, 2008, pp. 2800–2804.
[46] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): Status, results, and challenges," *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, Aug. 2012.
[47] J. Wang, Y. Liu, X. Liu, and J. Zhang, "A trust propagation scheme in VANETs," in *Proc. IEEE Intell. Veh. Symp.*, 2009, pp. 1067–1071.
[48] T. Gazdar, A. Rachedi, A. Benslimane, and A. Belghith, "A distributed advanced analytical trust model for VANETs," in *Proc. GLOBECOM*, 2012, pp. 201–206.
[49] Y. Xiang, Z. Liu, R. Liu, W. Sun, and W. Wang, "GeoSVR: A map-based stateless VANET routing," *Ad Hoc Netw.*, vol. 11, no. 7, pp. 2125–2135, Sep. 2013.

Zhiquan Liu received the B.S. degree from the School of Science, Xidian University, Xi'an, China, in 2012, and the Ph.D. degree from the School of Computer Science and Technology, Xidian University in 2017.

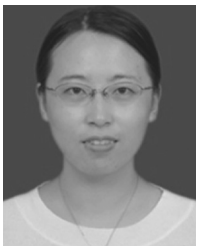
He is currently a Lecturer with the College of Cyber Security, Jinan University, Guangzhou, China, and his current research focuses on trust modeling and privacy protection in Internet of Vehicles.

Jian Weng received the B.E. and M.E. degrees from the School of Computer Science and Technology, South China University of Technology, Guangzhou, China, in 2000 and 2004, respectively, and the Ph.D. degree from the School of Computer Science and Technology, Shanghai Jiaotong University, Shanghai, China, in 2008.

He is currently a Professor with the College of Cyber Security, Jinan University, Guangzhou, and his research interests include cryptography, information security, and artificial intelligence.

Jianfeng Ma received the M.E. degree from the School of Computer Science and Technology, Xidian University, Xi'an, China, in 1988, and the Ph.D. degree from the School of Information and Telecommunication Engineering, Xidian University in 1995.

He is currently a Professor with the School of Cyber Engineering, Xidian University, and his current research interests include information security, coding theory, and cryptography.



Jingjing Guo received the M.E. and Ph.D. degrees from the School of Computer Science and Technology, Xidian University, Xi'an, China, in 2012 and 2015, respectively.

She is currently a Lecturer with the School of Cyber Engineering, Xidian University. Her current research focus on trust management, social network, access control, and information security.

Bingwen Feng received the B.E. and Ph.D. degrees from Sun Yat-sen University, Guangzhou, China, in 2008 and 2014, respectively.

He is currently a Lecturer with the College of Cyber Security, Jinan University, Guangzhou, and his research interests include multimedia security, network security, and privacy protection.

Zhongyuan Jiang received the B.E. and Ph.D. degrees from Beijing Jiaotong University, Beijing, China, in 2009 and 2013, respectively.

He is an Associate Professor with the School of Cyber Engineering, Xidian University, Xi'an, China, and his current research focuses on complex network, urban computing, and network security.

Kaimin Wei received the B.E. degree from Yuncheng University, Yuncheng, China, in 2007, and the M.E. and Ph.D. degrees from Beihang University, Beijing, China, in 2010 and 2014, respectively.

He is currently an Associate Professor with the College of Cyber Security, Jinan University, Guangzhou, China, and his research interests include mobile network and network security.