CATE: Cloud-Aided Trustworthiness Evaluation Scheme for Incompletely Predictable Vehicular Ad hoc Networks

Jian Shen, Chen Wang, Jin-Feng Lai, Yang Xiang, and Pan Li

***Abstract*—Incompletely predictable vehicular ad hoc networks (IPNs) are presented for vehicular networks with vehicles moving in particular ranges. A group of vehicles in the same region are required to encrypt and sign the uploaded region information in IPNs. So far, research has not been able to provide an appropriate trustworthiness evaluation system ensuring security and fairness in IPNs. In this paper, we first establish an evaluation system for vehicles in the network for secure and fair trustworthiness evaluation. Various vehicle attributes are utilized to evaluate the trustworthiness level of a vehicle. The novel trustworthiness evaluation can provide a more comprehensive and real-time update of vehicle status. Second, based on the system, we propose a cloud-aided trustworthiness evaluation (CATE) scheme. According to the evaluation results provided by the system, the CATE scheme also guarantees lightweight trustworthiness level confirmation with the help of session key generation. Besides, the information upload security is ensured with group signature and encryption. The security proof indicates that the proposed CATE scheme is secure for vehicles in IPNs to interact with trustworthiness. According to quantitative comparative analysis and experimental simulation based on paring-based cryptography (PBC) library, the designed scheme has been proved to be efficient.**

***Index Terms*—Incompletely predicable networks, cloud, trustworthiness evaluation, security.**

I. Introduction

MOBILE ad hoc networks have recently become widely applied in practice. Numerous outstanding schemes have been presented to provide a more reliable and secure network environment. However, many theoretical concepts cannot be applied to practical applications. Thus, reliability and security have aroused increased concern among researchers in the field of network computing and security [1], [2]. Some studies have focused on the predictability of node movement in such networks. A new type of network called incompletely predictable ad hoc networks (IPNs) was proposed in [3] to describe networks whereby individuals move around their basic positions or with a particular tendency. Nodes in such networks move in particular manners. The primary feature of IPNs is that a simple structure is used to describe the whole network. The purpose of an IPN model is to seek invariable elements in dynamic networks [4]. Thus, IPNs have recently generated considerable research interest in the fields of smart homes, smart medical and health research, meteorological monitoring and vehicular networks. Specifically, vehicular ad hoc networks (VANETs) are suitable for IPN models in many aspects. For instance, cars in an urban area, especially taxis, travel in a limited area for their own purposes or travel with tendencies that seldom change. We consider networks, such as taxi systems, as typical IPNs. Road-side units (RSUs) are not considered in IPN models. Region representative (RR), which is also a member of the vehicles in a certain region, is utilized as a regional signature and information aggregator.

Given the increased pace of urbanization, all types of cars are becoming widespread across cities. Each car, especially taxis in cities, usually has its own active range or known trajectory. These characteristics of vehicle networks determine that they can be defined as IPNs. In these networks, cars in the same region upload traffic information sharing situations of roads. To ensure the security of vehicle networks, the trustworthiness levels of cars in a region or those of a newcomer should be evaluated because the region cannot determine whether the vehicle is believable for information upload purposes. The evaluation system requires a composition of powerful computation and storage capabilities for data processing, information retrieval and fair trustworthiness evaluation. To achieve this, a trusted third party is required to provide the trustworthiness level of a vehicle who will join the region. Due to the requirements on reliability and security, a vehicle network scheme must be established with the assistance of the cloud to achieve efficient message authentication and data synchronization. Cloud computing is a new technique for distributed computing and provides storage services for the outsourced data of cloud users [5], [6], [7], [8], [9]. However, no technologies exist to ensure full trust on the cloud. Considering that an unfair evaluation might be made, a novel trustworthiness evaluation scheme needs to be composed considering vehicle confirmation to guarantee that the cloud serves as a semi-trusted third-party evaluator and a traffic information distribution center [10], [11], [12], [13].

Motivation for this work: There are still many unresolved problems in terms of trustworthiness in IPNs and vehicular

J. Shen and C. Wang are with the School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing, China. State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100878, China. E-mail: {s_shenjian, wangchennuist}@126.com

J.-F. Lai is with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, China. E-mail: lcf2018@uestc.edu.cn

Y. Xiang is with the Digital Research & Innovation Capability Platform, Swinburne University of Technology, John Street, Hawthorn, Victoria 3122, Australia. E-mail: yxiang@swin.edu.au

P. Li is with the Department of Electrical Engineering and Computer Science, Case School of Engineering, Case Western Reserve University, USA. E-mail: lipan@case.edu

Manuscript received XXX, XX, 2019; revised XXX, XX, 2019.

networks, although many trustworthiness methods and protocols have been presented for vehicles by researchers. Current trustworthiness methods lack a complete system for ensuring the fairness of the evaluation level. Unfair evaluations made by a malicious cloud need to be avoided. Most trustworthiness methods for vehicular networks require vehicles to upload local information. Unfortunately, few methods have considered the trustworthiness of the uploaded information. If a malicious region member provides incorrect messages or data that has been intentionally tampered with to the cloud, traffic congestion might occur in the region due to the use of incorrect information. More seriously, road rescue efforts may be delayed because of the provided incorrect information, which could affect people's lives and property. In addition, sensors on vehicles suffer from limited energy storage and computation capabilities. The sensors' batteries may need to be replaced prematurely due to the high computational complexity, causing substantial inconvenience to users. Therefore, a complete trustworthiness evaluation system is required to make sure the trustworthiness of members participating in information upload. Besides, a security scheme is needed to protect the trustworthiness evaluation results and safely uploaded information. Moreover, the operations performed by the vehicle sensors are required to be as lightweight as possible.

A. Our Contributions

In this paper, based on a novel designed trustworthiness evaluation system, a cloud-aided trustworthiness evaluation (CATE) scheme is presented to solve problems facing incompletely predictable vehicular ad hoc networks. The scheme can ensure secure and reliable information upload. The main contributions of this paper can be summarized as follows:

- **A secure and fair trustworthiness evaluation system is presented.** Assisted by the cloud, the system provides a reasonable assessment of a vehicle's condition according to its various attributes and considers the effect of time on the credibility of this assessment result. Note here that for fairness, the cloud is only responsible for data analysis and vehicle evaluation. The trustworthiness level provided by the cloud should be confirmed by the vehicle to prevent a malicious cloud server from making an improper evaluation. The decision to accept a vehicle should be made by the region representative.
- **Authenticated information upload is guaranteed.** Region-based traffic information is particularly important in vehicle networks. To ensure the privacy of uploaded information, this information needs to be acknowledged by all members of the region. Joint information certification in our scheme can ensure both the security and trustworthiness of the uploaded information.
- **Lightweight trustworthiness level confirmation by vehicles is achieved.** A vehicle has no need to do a large amount of computation to obtain other's trustworthiness in this scheme. The scheme avoids large-scale data analysis of vehicles. In determining whether to accept a newcomer, the region representative only needs to request the user's trustworthiness level from the cloud, rather than perform the evaluation calculations itself. When confirming the trustworthiness level evaluated by the cloud, a vehicle only needs to consider whether it is within its acceptable range, rather than having to re-evaluate its own attributes to ensure that the cloud has not maliciously evaluated the vehicle itself.

B. Related Work

IPNs are a type of ad hoc network. The most significant feature of IPNs is that vehicles in networks move in a certain range or following a particular rule. VANETs are a good example of IPNs. Various trustworthiness methods have been proposed to solve trust problems in VANETs when vehicles need to communicate or exchange information with each other. We divide these methods into three categories: entity-oriented trust methods, data-oriented trust methods and hybrid trust methods. Entity-oriented trust methods focus on presenting methods for ensuring that the communication between individuals is trustworthy. Data-oriented trust methods focus on evaluating the trustworthiness of the data transmitted on networks. Hybrid trust methods consider the trustworthiness of both entities and data.

Entity-oriented trust methods: Hao $et\ al.$ [14] proposed security protocols to detect compromised RSUs and their colluding malicious vehicles. They established a distributed key management framework to revoke the rights of malicious vehicles. The key distribution protocol presented in their paper was claimed to be able to prevent RSUs from misbehaving. Chen $et\ al.$ [15] proposed a beacon-based trust management system to resist internal attacks from sending false messages in VANETs. Additionally, the system enhances the location privacy of VANETs. Shaikh $et\ al.$ [16] presented an intrusionaware trust model for vehicular ad hoc networks. The model was proven to be robust and fault tolerant in their paper. Dias $et\ al.$ [17] presented a system utilizing a cooperative watchdog to detect and respond to malicious vehicles. They proved that their system can reduce the impact of misbehaving vehicles. Kerrache $et\ al.$ [18] presented a riskaware trustbased architecture to ensure multi-hop broadcast communication for both vehicle-to-vehicle and vehicle-to-RSU messages. However, these methods lack reasonable evaluation mechanisms for their trustworthiness. Moreover, a discussion on information upload privacy was also omitted in their paper.

Data-oriented trust methods: Raya $et\ al.$ [19] believed that data-oriented trust may be more appropriate in the domain of ephemeral ad hoc networks such as VANETs. They treated the trust of the entities as only one of the default parameters for data trustworthiness. The trustworthiness of the data changes frequently based on network and perceived environment changes. Additionally, the data source is unlimited or application dependent. Additionally, in their method for trustworthiness, the data are derived from multiple pieces of evidence from all types of parts of the network. However, this method does not explore data integration and reuse.

Hybrid trust methods: Park $et\ al.$ [20] presented a long-term reputation system for VANETs based on a vehicle's daily

commute routine. In this system, a virtual community is established by the daily commuting vehicles passing through RSUs. In addition, only a secret and verifiable certificate is needed for each vehicle in this system. Timpner $et\ al.$ [21] proposed a distributed and dynamic approach to establish trusted groups of vehicles. State-of-the-art encryption, signature algorithms and mathematical trust rating model are combined to achieve high performance. However, these methods need to be improved to satisfy the lightweight computing requirements.

Other researchers have focused on secure communication schemes for VANETs without consideration of trustworthiness. Horng $et\ al.$ [22] presented a group communication protocol called SPECS designed for secure authentication and data transmission for VANETs. However, although the SPECS scheme is efficient in vehicle authentication and data upload, it lacks a trustworthiness evaluation process for every vehicle and is not lightweight enough.

There are still numerous open issues in this field such as untrusted vehicle evaluation, incorrect local data upload and heavy computational burden. Based on existing studies, to further improve the method of establishing trustworthiness in IPNs, we consider the cooperation among entities, the integration of various data sources and the hybridization of advanced technologies.

C. Organization

The remainder of this paper is organized as follows. Section 2 presents some preliminaries, including the concept of IPNs, bilinear pairing and the complexity assumption of this paper. Section 3 presents the novel trustworthiness evaluation system. Section 4 shows the security models of the CATE scheme. Section 5 gives the detailed process of the CATE scheme. Section 6 states the security analysis and simulation results. Finally, the conclusions are drawn in Section 7.

II. Preliminaries

To better demonstrate our scheme, we present some preliminaries, including the definitions of IPNs, bilinear pairings and the complexity assumption. Explanations of these concepts are presented here. Some notations utilized in our scheme are listed in Table I.

A. IPNs

IPNs evolved from traditional network types. Delay-tolerant networks (DTNs) [23], [24], wireless mesh networks (WMNs) and wireless sensor networks (WSNs) [1], [25] are well known time-evolving and predictable networks. This type of network is shown in Fig. 1. Fig. 1 intends to illustrate the situation whereby in vehicular networks, cars move with a particular tendency or in a specific range in a city. We model the topology constructed by the vehicles as a space-time graph. In social networks, the node mobility can be predicted with a potential accuracy of approximately 93 percent [26]. Moreover, there is a special situation in which the node positions and the link statuses are fixed. IPNs are a suitable tool for modeling VANETs in these cases, and we treat IPNs as the basis of the novel scheme for the trustworthiness evaluation.

TABLE I: Notations in our scheme

Symbol	Description
$\mathfrak{a}_m$	The m-th trustworthiness attribute information (TAI) value of a vehicle
$\mathfrak{A}$	The set of TAI values
$\mathfrak{w}_i$	The weight of the i-th TAI
$\mathfrak{E}$	The trustworthiness level (TL) value
$\mathfrak{E}^{inst}(t)$	The instantaneous TL value of a vehicle at time t
$\mathfrak{E}(t^-)$	The previous TL value
δ	The value $\mathfrak{E}(t^-)$ should be accounted for
Δt	The time interval between time t and time t^-
θ	A constant utilized to control the annealing speed of the previous TL value
$\mathfrak{O}$	The output of the TL confirmation
NC	Newcomer in a region
RR	Region representative
γ	Confirmation message
R	A region
$info_R$	The encrypted information of region R
P, Q	Points of $\mathbb{G}_1$

In Fig. 1, vehicles form different regions, which are represented by doted circles when the vehicles are moving. The traffic information possessed by each vehicle in a given region can be collected to represent the overall situation of that region. Over time, the locations of vehicles change, resulting in changes in region divisions. In the IPN model of this paper, region representatives (RR) are selected to replace the RSUs in traditional VANETs. The regions of the network are predetermined when the network is initialized according to the network topology. Due to the page limitation, the detailed definition of IPNs is ignored in this paper. For more details, please refer to [27].

B. Bilinear Pairing

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two groups of the same prime order q. Let $\mathbb{G}_1$ be an additively written group, and let $\mathbb{G}_2$ be a multiplicatively written group. Given a mapping e, a bilinear pairing on $(\mathbb{G}_1, \mathbb{G}_2)$: $\mathbb{G}_1^2 \rightarrow \mathbb{G}_2$ satisfying the following properties is called a cryptographic bilinear map.

Bilinearity. $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1$and $a, b \in Z_q^*$. This can be expressed in the following manner. For $P, Q, R \in \mathbb{G}_1$, $e(P + Q, R) = e(P, R)e(Q, R)$ and $e(P, Q + R) = e(P, Q)e(P, R)$.

Non-degeneracy. If P is a generator of $\mathbb{G}_1$, then $e(P, P)$ is a generator of $\mathbb{G}_2$. In other words, $e(P, P) \neq 1$.

Computability. e can be efficiently computed.

C. Complexity Assumption

Our complexity assumption is based on Gap-Diffie-Hellman (GDH) groups. Let $\mathbb{G}_1$ be a multiplicative group of prime order p. We consider the following two problems in $\mathbb{G}_1$.

Computational Diffie-Hellman (CDH) problem. Take an instance as (P, aP, bP) for some $a, b \in Z_q^*$. Output abP.

Decisional Diffie-Hellman (DDH) problem. Take an instance as (P, aP, bP, cP) for some $a, b, c \in Z_q^*$. Output "yes" if $c = ab \mod q$ and "no" otherwise. The DDH problem in $\mathbb{G}_1$ can be solved in polynomial time by verifying $e(aP, bP) = e(P, cP)$.

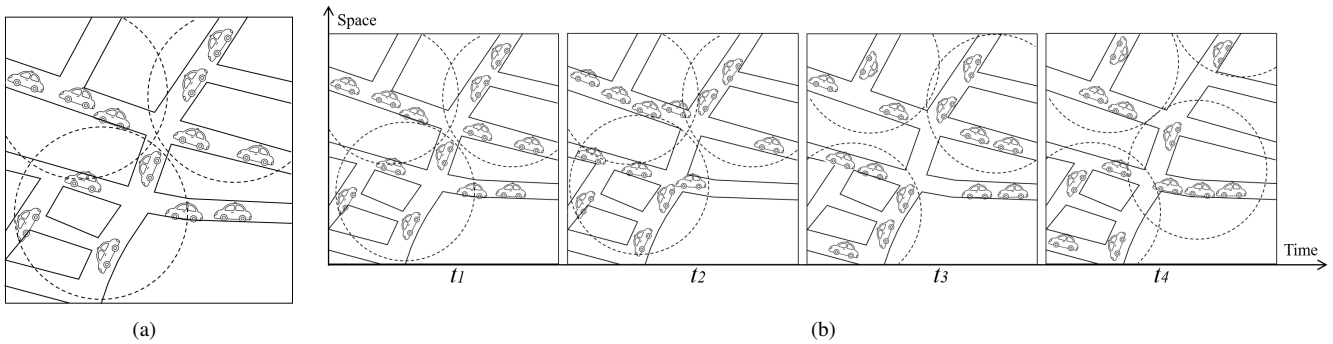

Fig. 1: An example of IPNs: (a) a snapshot of the network and (b) time-evolving topologies of vehicles in IPNs.

Gap-Diffie-Hellman (GDH) group. A prime order group $\mathbb{G}_1$ is a GDH group if there exists an efficient polynomial-time algorithm that solves the DDH problem in $\mathbb{G}_1$ and if there is no probabilistic polynomial-time algorithm that solves the CDH problem with non-negligible probability of success.

III. A Novel Trustworthiness Evaluation System

Before detailing the CATE scheme, a novel trustworthiness evaluation system is presented in this section. The CATE scheme requires a sound trustworthiness evaluation system to ensure that all regional participants are acceptable. Dividing vehicles into different categories or levels according to their unique attributes is one of the main methods of determining the trustworthiness of these vehicles. By combining with a cloud environment, a trusted third party represented by the cloud is utilized to perform the vehicle trustworthiness evaluation. Meanwhile, using distributed cloud storage technology to store the trustworthiness attribute information of different periods ensures the integrity and security of the data.

In this section, we provide some important definitions for our proposed trustworthiness evaluation system. According to these well-defined concepts, the process underlying the novel trustworthiness evaluation system is stated.

A. Important Concepts for the System

For a more detailed exposition of the novel trustworthiness evaluation system, we first define two new concepts: trustworthiness attribute information (TAI) and trustworthiness level (TL).

Definition 1 provides the meaning of TAI.

Definition 1 (Trustworthiness attribute information, TAI): TAI represents various attribute parameters of an individual utilized to perform a trustworthiness evaluation of that individual. TAI is not a single value but rather is a collection of parameters obtained by sensor nodes on the vehicle. Set $\mathfrak{A} = \{\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, ...\mathfrak{a}_m\}$, where $\mathfrak{A}$ represents the set of TAI, and $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, ...\mathfrak{a}_m$ denote different parameters collected by m sensors to reflect the attributes of the vehicle. In our system, these values are signed by sensors and cannot be changed by the user himself.

Clearly, TAI is the personal information of a given vehicle, therein containing private data collected by sensors on the vehicle. TAI may include the up-to-date active state, running time, mileage, fuel consumption, driving tracks, traffic accident records, and other parameters that can reflect the vehicle health status and behavior patterns. TAI only records data faithfully, as opposed to performing data analysis.

The purpose of collecting TAI is to enable the cloud server to perform TL evaluations. A description of the TL is presented in Definition 2.

Definition 2 (Trustworthiness level, TL): The TL is an evaluation standard provided by the cloud server, according to the TAI uploaded by the vehicle and other information.

The TL varies according to the status of the vehicle. Pouryazdan $et\ al.$ [28] presented a vote-based trustworthiness management system. Every vehicle in the system has the opportunity to vote for the newcomer. The TL value is denoted as $\mathfrak{E}$. Eq. (1) provides the instantaneous TL value $\mathfrak{E}^{inst}(t)$ of a vehicle at time t.

$$\mathfrak{E}^{inst}(t) = \frac{\sum_{i=1}^{m} \mathfrak{w}_i \mathfrak{a}_i}{m} \tag{1}$$

where $\mathfrak{w}_i$ is the weight of the i-th TAI. Note that, the weight value should be carefully selected so that each parameter change can be reflected in the TL value. In addition, the weight value is mainly utilized to determine whether a parameter is positively or negatively correlated with the TL value. $\mathfrak{E}^{inst}(t)$ is the weighted mean of the m attributes contained in $\mathfrak{A}$.

The TL is not a constant value for complex vehicle networks. The TL needs to be adjusted dynamically over time based on the up-to-date status of the vehicle. The integrated TL value $\mathfrak{E}(t)$ at the end of a time period t is formulated in Eq. (2). $\mathfrak{E}(t)$ is the weighted sum of the instantaneous TL value $\mathfrak{E}^{inst}(t)$ and the last integrated TL value $\mathfrak{E}(t^-)$ recorded in the cloud at time t^-.

$$\mathfrak{E}(t) = \left(1 - \frac{\delta}{\theta \cdot (1 + \Delta t)}\right) \cdot \mathfrak{E}^{inst}(t) + \frac{\delta}{\theta \cdot (1 + \Delta t)} \cdot \mathfrak{E}\left(t^-\right) \tag{2}$$

where δ indicates that the previous TL value $\mathfrak{E}(t^-)$ should be accounted for. This proportion varies over time. Δt is the time interval between time t and time t^-. θ is utilized to control the annealing speed of the previous TL value. Over time, the reference value of the previous TL value decreases. If the interval is long enough, the TL value at time t ($\mathfrak{E}(t)$) will depend entirely on the current vehicle condition.

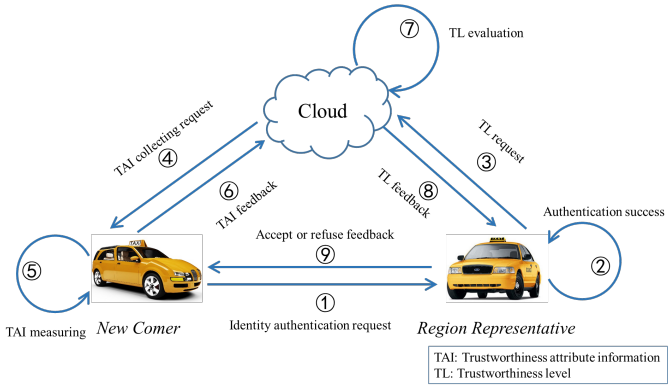

Fig. 2: The trustworthiness evaluation system.

In general terms, the new design of the evaluation system involves the utilization of a cloud server to help achieve the evaluation of the user trustworthiness level, which is represented by the TL in Definition. 2. Users simply need to upload their own TAI to the cloud. The cloud server is in charge of the calculation of users' TL values, and the region only needs to make "accept" or "reject" decisions.

If the vehicle is in good condition (for example, short running time, low fuel consumption of the vehicle and no traffic accident records, etc.) and the cloud can obtain traffic information from it for a long period of time, a high TL evaluation will be made by the cloud. A satisfactory state of a vehicle means that the parameters show that the vehicle is in good condition and suitable for the transmission of road condition information in the designed protocol. If the state of the vehicle is not satisfactory, then the cloud will provide a bad TL evaluation based on its status. This evaluation will determine whether the system will accept the traffic information uploaded by the vehicle.

B. The Evaluation System Process

This evaluation system is essential to the realization of the entire scheme. The main function of the evaluation system aided by the cloud is to analyze the data of all periods for the user from various aspects and to provide a suitable TL value for the user. This process is generally performed in a region when personnel changes occur. Therefore, we first take the evaluation of a newcomer as an example to illustrate this evaluation process.

The example of a situation whereby a newcomer joins a region is used to illustrate the operation of our proposed system of trustworthiness evaluation. Note that, in our system, the computing resource of the cloud is considered to be infinite. When a vehicle travels into an area and decides to join this region and help the region collect and upload region information, our system performs nine steps, as illustrated in Fig. 2, to evaluate the newcomer. The nine steps are listed as follows:

Step 1 The newcomer in the region sends its identity to the region representative (RR). We assume that the ID of the newcomer is "NC". This ID message has two functions. First, the representative searches a local blacklist to determine whether the newcomer is a clean user. Second, the identity information is used to map the correct TL value to the associated vehicle.

Step 2 The region representative has received the identity information "NC". The identity of the newcomer is authenticated by the region representative according to the identity information. If the vehicle is a clean vehicle, the process will continue.

Step 3 The region representative makes a request to the cloud server for the TL of the newcomer, whose ID is "NC".

Step 4 The cloud server issues a request to the corresponding newcomer to collect its TAI.

Step 5 The newcomer measures and collects its own attribute data using a variety of sensors. These data will be written into the TAI and labeled with "NC".

Step 6 The new user feeds back the TAI to the cloud.

Step 7 The cloud server performs the TL evaluation according to various parameters in the TAI, as detailed in Section III-A. The latest TL value of "NC" at this moment is obtained and stored by the cloud.

Step 8 The cloud sends the TL to the region representative.

Step 9 The region representative responds to the request of the newcomer for acceptance or rejection given the TL value provided by the cloud and the TL requirement of this region. Note that TL requirements of regions in a VANET are usually invariable, while the RR can refine the access rule according to characteristics of the region. For example, in complex traffic sections, the RR may change the access rule so as to increase the TL requirement of the region. As a consequence, only reliable vehicles with high trustworthiness can participate in road data acquisition.

Although the above nine steps describe the overall process of the evaluation system, the adjustment of the step order and the choice of steps are subject to change given specific circumstances. First, for instance, a newcomer can immediately upload the TAI to the cloud when it is going to join the region. When the region representative asks the cloud for the TL of that vehicle, the cloud decides whether to let the vehicle provide new TAI again based on the timestamps of the previously uploaded TAI and the TL request of the region representative. Second, the confirmation of the TL value provided by the cloud will be implemented by the newcomer itself to ensure that the cloud has not maliciously provided a biased evaluation. In addition, when vehicles participate in the region, they need to perform local information upload together. Note that, after the TL value of a vehicle is calculated, it will be used to determine whether the vehicle satisfies the entry requirement of a certain region. All the historical TL values will be stored in the cloud server for subsequent TL value calculation.

In addition, the situation of only a single vehicle in a region will happen when other vehicles in the same region leave. The single vehicle in the region is automatically selected as the RR of the region. Besides, a single vehicle that is not in any region cannot automatically form a region, since there is no corresponding RR to approve its entry. The RR must be

selected in vehicles in the region and responsible for vehicle entry in a period of time. When its round ends, the system automatically selects another node in the same region as the next round RR. In our system, every region must have an RR.

C. System Advantages

A vehicle trustworthiness evaluation system supported by a cloud server is proposed. The system utilizes the data processing and storage capacity of the cloud to decentralize the evaluation rights to different parts of the system to ensure the high efficiency and privacy of the operation. The above system has the following advantages.

- **Privacy protection:** The system can prevent a region representative from obtaining the TAI of the newcomer. This is because the TAI contains private information about the newcomer. There is a risk that personal information could be leaked to the region representative if the TAI is directly transmitted to the representative.
- **Resource savings:** By fully utilizing the cloud computing and storage resources, cars can save computing and storage resources when the trustworthiness level is required. The region representative does not need to address the vast attribute information of the newcomer. Moreover, the cloud can help speed up the process for the entire system. A newcomer can upload its TAI to the cloud at any time. Thus, the TL value can be calculated in advance by the cloud and sent to the region representative at the moment that he asks for the TL value of the newcomer.
- **Subsidiarity:** The cloud has no right to decide whether the newcomer can or cannot be accepted based on the information that the user uploads to the cloud. Referencing the TL of the newcomer, the region representative has the power to decide whether the region should grant the newcomer membership. This can ensure that the region can select the correct member given its own situation. In addition, the cloud cannot arbitrarily change the user's TL evaluation; in other words, any TL evaluation should be acceptable to the user.

IV. Security Models

The CATE scheme is proposed based on the novel evaluation system. In this scheme, an adversarial cloud server may attempt to tamper with or forge the evaluation results for a specific vehicle. An adversarial region representative may attempt to forge some of the members in its region. Moreover, an adversarial outsider may pretend to be a member of the region and upload incorrect local information. Here, we provide the security models utilized for the CATE scheme in terms of an adversarial cloud server, adversarial region representative and adversarial outsider. It is worth noting that once a vehicle enters into a certain region with the approval of the RR, it is considered as a secure and trustworthy one.

A. Adversarial Cloud Server

In the scheme, the cloud is solely responsible for evaluating the TL and providing TL values, which may lead to misjudgments. We consider that every vehicle has its own acceptable TL value interval. An adversarial cloud server may provide an inappropriate TL value for a user, which can lead to some trusted users being rejected by the region due to their low TL values or some untrusted vehicles being accepted because of their high TL values. A user may lose a chance to "socialize", which may result in issues in future trustworthiness evaluations. The region may also lose an honest data collector. The concept is established to prevent such a situation from occurring. Therefore, to satisfy the security requirement, the concept of *One-More-Unforgeability under Chosen Message Attack* (OMU-CMA) is defined as follows.

Definition 3 (OMU-CMA): The OMU-CMA game is defined as

Setup. The adversary $\mathcal{A}$ is given the TL value τ. The challenger runs the TLC-KeyGen algorithm to obtain the key pairs (P_{sk}, P_{pk}) of the target vehicle v_t and provides the public key P_{pk} to the adversary.

MC-Query. The adversary $\mathcal{A}$ can adaptively query the challenger for the signature x_t for at most q_k distinct original messages of his choice $m_1, m_2, ..., m_{q_k}$ through the protocol. The challenger responds to the adversary with messages signed by v_t.

Output. Finally, the adversary outputs x_t and the confirmation message $\gamma = xH(\tau)$. If the final validation algorithm results in a "pass", the adversary $\mathcal{A}$ wins the game.

We refer to such an adversary $\mathcal{A}$ as an OMU-CMA adversary and define its advantage $\mathrm{Adv}^{\mathrm{OMU-CMA}}_{\mathcal{TLC},\mathcal{A}}(\lambda)$ to be the probability that $\mathcal{A}$ wins the game.

B. Adversarial Region Representative

An adversarial region representative may want to implement joint information certification without a designated user. It is possible that a vehicle in a region will be forged by an adversarial region representative, causing some cloud-authenticated messages to not be signed by all members of the region. For that reason, the concept of security for joint information certification has to prevent this from occurring. In other words, no valid multi-signature should keep an honest vehicle that is part of a region R accountable if it did not participate in signing.

In this security model, the adversary is allowed to generate the corrupted users' public and private keys with the help of a key generation algorithm. The adversary is allowed to corrupt almost all vehicles. The goal of the adversary is to forge the only remaining honest vehicle.

To best satisfy such a security requirement, we define the concept of *Against Existential Forgery under Chosen Message Attack* (AEF-CMA) as follows.

Definition 4 (AEF-CMA): The AEF-CMA game is defined as follows.

Given a single honest vehicle v_1, the adversary $\mathcal{A}$ owns the public key of v_1. Given the remaining $r-1$ vehicles of that region, the adversary $\mathcal{A}$ owns $r-1$ pairs of public and secret keys corresponding to the $r-1$ corrupted vehicles who need to certify the region information. The adversary $\mathcal{A}$ provides a message-subgroup-signature triple $(info_R, R, \sigma)$ and runs the verification algorithm. If the output is "1", $\mathcal{A}$ wins the game.

We consider such an adversary $\mathcal{A}$ aforementioned in the game as an AEF-CMA adversary and define its advantage $\mathrm{Adv}_{\mathcal{RV},\mathcal{A}}^{\mathrm{AEF-CMA}}(\lambda)$ to be the probability that $\mathcal{A}$ wins the game.

C. Adversarial Outsider

An adversarial outsider is a user who does not belong to a region but is eager to obtain information about that region. We assume that an attacker can obtain information that has not been signed by the region members after being encrypted.

The concept of *Region Identity-based Indistinguishability under adaptive Chosen Message Attack* (IND-RID-CMA) is defined as follows to satisfy such a security requirement.

Definition 5 (IND-RID-CMA): The IND-RID-CMA game is defined as follows.

Setup. The challenger generates key pairs $(P_{pub_{\mathcal{CS}}}, \beta_{\mathcal{CS}})$. The public key $P_{pub_{\mathcal{CS}}}$ is provided to the adversary $\mathcal{A}$, and the secret key $\beta_{\mathcal{CS}}$ is kept by the challenger.

Query-I. $\mathcal{A}$ queries at most q_k distinct region identities R_{ID}, denoted $R_{ID_1}, ..., R_{ID_k}$. The challenger runs the RV-ENCRP algorithm, generates the corresponding private key f_R and sends the key to $\mathcal{A}$. Then, the challenger runs the RV-DNCRP algorithm to decrypt the ciphertext $info_R$ using the private key f_R. The plaintext will be sent to the adversary $\mathcal{A}$.

Challenge. The attacker sends the challenger two equal-length plaintexts m_0 and m_1 and a region identity R_{ID_q} on which the attacker wishes to be challenged but that did not appear in Query-I. The challenger picks $b \in_R \{0,1\}$ and computes $info_{R_q} = \text{RV-ENCRP}(R_{ID_q}, m_b)$. $\mathcal{A}$ will receive $info_{R_q}$ as the challenge.

Query-II. The attacker continues the query $q_{k+1}, ..., q_n$ about the region identity R_{ID}s and ciphertexts, except for R_{ID_q} and $info_{R_q}$.

Output. Finally, the adversary $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$ and wins the game if $b = b'$.

We refer to such an adversary $\mathcal{A}$ as an IND-RID-CMA adversary. We define adversary $\mathcal{A}$'s advantage in attacking the concept with the advantage described as $\mathrm{Adv}_{\mathcal{RV},\mathcal{A}}^{\mathrm{IND-RID-CMA}}(\lambda) = \Pr[b = b'] - 1/2$.

According to the discussed security models, we perform security analysis for the proposed CATE scheme.

V. The Proposed CATE Scheme

This section attempts to clarify the details of the CATE scheme. First, we present an overview of this scheme. Subsequently, based on the presented evaluation system, we discuss the security methods of the CATE scheme with regard to three aspects: newcomer-representative authentication (which is described in system step 1), trustworthiness level confirmation (which is a complement of the system to ensure the fairness of the evaluation result), and joint information certification (which is the main function of the CATE scheme utilized by members in the same region to upload local information).

A. An Overview of CATE

CATE is a trustworthiness evaluation scheme designed for incompletely predictable vehicular ad hoc networks. CATE utilizes the presented novel trustworthiness evaluation system for vehicles in a region. Meanwhile, all the individuals in the region jointly certify the authenticity of a document and upload the authenticated message to the cloud. Fig. 3 illustrates the entire model of the scheme.

In detail, the large circles are the different regions. The hollow circles in the regions represent common vehicles, while the solid circles represent the region representative of a certain region in the network. Fig. 3 is a schematic diagram, where the locations of the vehicles in the figure are symbolic representations. All the vehicles in the network can outsource their data to the cloud, a process that is unrelated to the positions of the vehicles in the schematic. The framework of the CATE scheme is a joint information certification based on trustworthiness evaluation. More specifically, given a network with all vehicles moving based on their own rules, the proper vehicle-to-vehicle routes for transmitting messages are found with the assistance of the cloud. This is because the joint information certification method ensures the accuracy of the uploaded area information. For instance, the trajectories of some people (such as civil servants) can be found regularly. Enough trajectory information can be collected to predict the movement of their vehicles. Once the network can predict the trajectory of each vehicle, it can plan the shortest path of V2V information transmission. Specifically, when entering a region, a newcomer is treated as a newcomer to the region. As shown in Fig. 3, a newcomer wants to participate in region 2. Not only does the region representative of the given region have to certify its identity, but the cloud also helps to evaluate its trustworthiness according to the attributes of the vehicle. The traffic information of a region is often consistent. Therefore, the members of a region would sign a document that would include information about the traffic data, which is called the joint information certification. The document would be uploaded to the cloud by the region representative. The implementation of the CATE scheme requires collaboration between the cloud, the region representatives and the common vehicles.

The entire CATE process can be summarized as newcomer authentication, trustworthiness evaluation and joint information certification. Newcomer authentication represents the process performed when a vehicle wants to join the region and sends a message to the region representative to authenticate its identity. Trustworthiness evaluation requires that a vehicle that needs to be evaluated upload its trustworthiness attribute information (TAI). Then, the cloud evaluates the vehicle and sends its TL value to the vehicle to confirm the TL value. Therefore, trustworthiness evaluation can be summarized as TAI upload, TL evaluation and TL confirmation. Note here that TL confirmation is implemented by the evaluated vehicle itself. Joint information certification represents the process whereby vehicles in the some region sign the same information together, and the information should be uploaded to the cloud. Theses three phases work together to complete the whole scheme. The relationship of the three phases is elaborated as follows. The TL value generated by the trustworthiness evaluation phase will be recorded as the reference basis for the judgment of the trustworthiness value in the newcomer

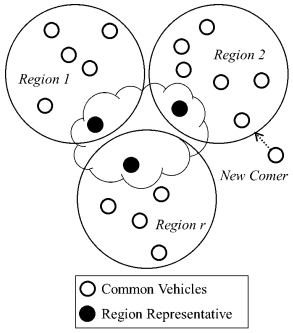

Fig. 3: The CATE scheme.

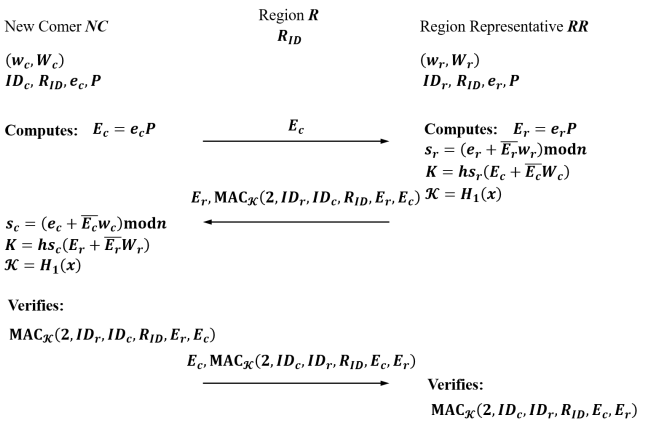

Fig. 4: Newcomer-Representative Authentication

authentication phase. The newcomer authentication phase will generate a new session key for a vehicle who comes into a new region. Note that the new session key will be utilized to transmit region information between the vehicles in the joint information certification phase. Finally, the information and confirmation will be signed by all members in the region and sent to the cloud server.

B. Newcomer-representative Authentication

In the proposed CATE scheme, when a vehicle enters a region, both the region representative and the vehicle are incapable of confirming each other's identity. On the one hand, the newcomer needs to determine whether he is going to enter the region that he wants to enter. On the other hand, the region representative needs to help the entire region determine whether the user can be a trusted partner. In other words, the two sides require mutual identification.

The authentication between the newcomer and the region representative can be implemented as follows.

Assume that the newcomer NC wants to join the region R and that he needs to perform authentication with the region representative RR. The detailed process is illustrated in Fig. 4. [29] utilized a similar method to achieve secure communication between a patient's controller and a healthcare worker's device. The authenticated key agreement method is proven to be secure [30]. A message authentication code algorithm, denoted MAC, such as HMAC, is required here to provide key confirmation. A key derivation function, $\mathcal{H}_1$ is required, taking SHA-1 as an example. Both NC and RR generate static key pairs (w_c, W_c) and (w_r, W_r) and ephemeral key pairs. To ensure that the entry region is correct, in addition to the newcomer ID ID_c and the region representative ID ID_r, the region ID R_{ID} is also utilized as part of the MAC message.

1) NC generates $e_c \in_R [1, n-1]$, computes the point $E_c = e_c P$ and sends it to RR.
2) RR computes the authentication message in the following four steps and sends it to NC.
   a) RR generates $e_r \in_R [1, n-1]$ and computes the point $E_r = e_r P$.
   b) RR computes $s_r = (e_r + \overline{E_r} w_r) \bmod n$ and $K = hs_r(E_c + \overline{E_c} W_c)$. If $K = \mathcal{O}$, RR terminates the protocol run with failure. $\mathcal{K}$ is the shared secret key.
   c) RR utilizes the x-coordinate value x of the point K to compute a shared key $\mathcal{K} = \mathcal{H}_1(x)$.
   d) RR computes $\mathrm{MAC}_{\mathcal{K}}(2, ID_r, ID_c, R_{ID}, E_r, E_c)$ and sends this and E_r to NC.
3) NC utilizes the message sent by RR to authenticate the identity of RR and computes its own authentication message for RR.
   a) NC computes $s_c = (e_c + \overline{E_c} w_c) \bmod n$ and $K = hs_c(E_r + \overline{E_r} W_r)$. If $K = \mathcal{O}$, NC terminates the protocol run with failure.
   b) NC utilizes the x-coordinate value x of point K to compute a shared key $\mathcal{K} = \mathcal{H}_1(x)$.
   c) NC computes $\mathrm{MAC}_{\mathcal{K}}(2, ID_r, ID_c, R_{ID}, E_r, E_c)$ and verifies that this equals what was sent by RR.
   d) NC computes $\mathrm{MAC}_{\mathcal{K}}(3, ID_c, ID_r, R_{ID}, E_c, E_r)$ and sends this to RR.
4) RR computes $\mathrm{MAC}_{\mathcal{K}}(3, ID_c, ID_r, R_{ID}, E_c, E_r)$ and verifies that this equals what was sent by NC.
5) The shared secret is K, where $K = hs_c(E_r + \overline{E_r} W_r) = hs_r(E_c + \overline{E_c} W_c) = hs_c s_r P$.

After performing the above steps, NC and RR have successfully authenticated each other. NC is considered as a legal entrant, and RR will ask the cloud for NC's TL value.

C. Trustworthiness Level Confirmation

Note here that the data storage and processing on the cloud are considered safe. However, in our security model, we cannot prevent the cloud from deliberately lowering a user's TL value to crowd out the user from the region or increasing a user's TL value to put the user into the region. To prevent this circumstance, we need the user to sign his TL evaluated by the cloud to prove that the evaluation is acceptable to him. A vehicle will refuse to accept the TL value if the value is not within its acceptable TL interval. If there is no user confirmation, the TL evaluation is invalid.

We now present the method that allows a user to judge whether the TL evaluation provided by the cloud is reasonable.

Each user determines the minimum acceptable TL evaluation value $\mathfrak{E}_{min}$ according to their own circumstances, the surrounding environment and other factors. When a user obtains a TL value $\mathfrak{E}(t)$ for a certain moment t, the user will

determine whether the TL value is within its acceptable range. The output is defined as $\mathfrak{O}$ in Eq. (3).

$$\mathfrak{O} = \begin{cases} 1, & \mathfrak{E}(t) \geq \mathfrak{E}_{min} \\ 0, & \mathfrak{E}(t) < \mathfrak{E}_{min} \end{cases} \tag{3}$$

When $\mathfrak{O}$ equals 1, the user signs this TL value and sends to the region representative. When $\mathfrak{O}$ equals 0, the TL value will not be sent, and the cloud will be asked to reanalyze the TL. The user has the right to give up joining the region at any time if the TL value cannot be accepted as satisfactory.

The region representative simultaneously accepts the TL value from the cloud and that signed by the user. The region representative verifies the validity of the signature and compares whether the two TL values are the same. If they are the same, the region representative decides whether to accept the user based on the TL value. This will prevent the cloud from performing malicious evaluations for the user while ensuring that the TL values are not tampered with by the user.

Once the cloud has computed the TL value of a user (such as the above-mentioned newcomer), in the above flow, the cloud will feed the TL value back to the region representative. According to the security model defined in this paper, the cloud may provide a false or tampered TL value to reduce the trustworthiness of the vehicle. Under this circumstance, the trust level may be too low to be accepted by the region. The region representative will determine whether to accept the user and regional information that the user provides according to the TL value disseminated by the cloud. The BLS short signature proposed in [31] and public key encryption method are utilized to achieve secure TL confirmation. First, we need to ensure the secure transmission of the TL value. Second, to confirm the vehicle's receptivity to the TL value, the vehicle is required to sign the value.

We define the TL confirmation method (TLC method) as **TLC** = (**TLC-KeyGen**, **TLC-Conf**, **TLC-Ver**). Three algorithms are utilized in this method. A random key generation algorithm **TLC-KeyGen** outputs a pair of a public key and a private key, which is utilized by the entity that wants to confirm its own TL value evaluated by the cloud. A randomized short signature algorithm **TLC-Conf** is run by some vehicles to sign its confirmation message. A deterministic verification algorithm **TLC-Ver** is run by the region representative to verify whether the evaluated vehicle has accepted the TL evaluation. Note here that the short signature scheme uses bilinear pairing and GDH groups. A concrete presentation of the method is presented as follows.

TLC-KeyGen. Let H: $\{0,1\}^* \rightarrow \mathbb{G}_1$ be a map-to-point hash function. The private key $x \in_R Z_q^*$ and the public key $X = xP$ are generated for a vehicle who wants to confirm the TL value. The cloud owns the private key $c \in_R Z_q^*$ and the public key $C = cP$. The region representative owns the private key $r \in_R Z_q^*$ and the public key $R = rR$. The cloud sends encrypted τ to both the evaluated vehicle and the region representative.

TLC-Conf. The vehicle receives the encrypted TL value and decrypts it. Given the private key x and the TL value $\tau \in \{0,1\}^*$, the vehicle computes the confirmation message $\gamma = x\tau$. The vehicle encrypts γ with the representative's public key R and sends it to the region representative.

TLC-Ver. Given the public key P_{pk}, a TL value τ and a confirmation message γ, the region representative verifies $(P, \gamma) = e(X, \tau)$.

Here, we present the proof of the correctness of the algorithm **TLC-Ver**:

$$e(P, \gamma) = e(P, P_{sk}H(\tau)) = e(P_{pk}, H(\tau))$$

The security of **TLC** is the same as BLS; therefore, the security analysis will not be detailed in this paper. The **TLC-Ver** algorithm will output "pass" if the equation holds; otherwise, it will output "fail".

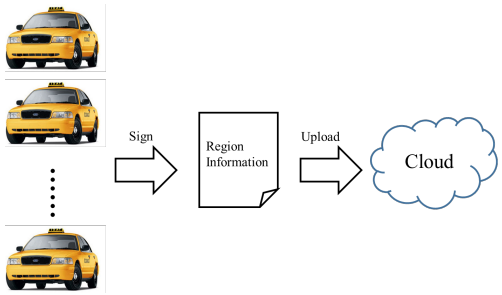

Fig. 5: Joint information certification.

D. Joint Information Certification

Region information is a carrier that the region utilizes to reflect the traffic situation and other related information of a certain region. The region uploads the region information file to the cloud after the file has been signed by all the members in this region. This process is visualized in Fig. 5.

The vehicles in Fig. 5 sign a document together, and the document containing the region information is uploaded to the cloud. This document needs to be signed by all regional members because the regional information summary is a real-time presentation of road conditions in the area, and no significant deviation is allowed. The regional information relates to the scheme for vehicle scheduling.

In our scheme, the local information needs to be uploaded to the cloud to facilitate system traffic scheduling, risk elimination, route planning, etc. Signatures are utilized to verify messages and represent a widely used public key encryption method [32]. To allow any subgroup of a group of users to jointly sign a message, Boldyreva *et al.* [33] developed a multi-signature scheme. The algorithms of a multi-signature scheme include a randomized key generation algorithm, a possibly randomized multi-signature generation algorithm and a deterministic verification algorithm. We improve the scheme for application in incompletely predictable vehicular ad hoc networks in Fig. 5.

The multi-signature scheme in [33] uses bilinear pairings and GDH groups.

For each subgroup across the entire network, defined as a region in this paper, we design a region vehicle information upload method (RV-IU method) **RV-IU** = (**RV-KeyGen**$_{CS}$,

RV-KeyGen, **RV-ENCRP**, **RV-MC**, **RV-Ver**, **RV-DECRP**). The method consists of six parts as follows. A randomized key generation algorithm of the cloud server **RV-KeyGen**$_{\mathcal{CS}}$ outputs its own public key and master private key, and it outputs the public and private keys specific to each region's identity. A randomized key generation algorithm **RV-KeyGen** outputs a pair of a public key and a secret key, which is utilized by the vehicles. This process is designed to be performed by every vehicle. An encryption algorithm **RV-ENCRP** is used to encrypt the region information. The randomized multi-signature creation algorithm **RV-MC** is an interactive protocol run by an arbitrary subset of the vehicles. This process is designed to be performed by the region representative. A deterministic verification algorithm **RV-Ver** is utilized to decide whether the information can be uploaded. A decryption algorithm **RV-DECRP** is used to decrypt the region information. The final two processes, the tasks of verification and data storage, are designed to be completed by the cloud server in the scheme proposed in this paper.

RV-KeyGen$_{\mathcal{CS}}$. A hash function H is chosen as $\{0,1\}^* \to \mathbb{G}_1$ and H_2: $\mathbb{G}_2 \to \{0,1\}^n$. The cloud server generates a pair of a public key and a private key $(P_{pub_{\mathcal{CS}}}, \beta_{\mathcal{CS}})$, which is valid only for this region R. $\beta_{\mathcal{CS}}$ is randomly picked by the algorithm, and $\beta_{\mathcal{CS}} \in_R \mathbb{Z}_q^*$. The public key is computed as $P_{pub_{\mathcal{CS}}} = \beta_{\mathcal{CS}} P$. Given a public region identity $R_{ID} \in \{0,1\}^*$, the public key $Q_R = H(R_{ID})$ and the private key $S_R = \beta_{\mathcal{CS}} Q_R$ are computed.

RV-KeyGen. Consider a set V of all n vehicles in the network. The algorithm then picks a random $\alpha_i \in_R \mathbb{Z}_q^*$. Each vehicle v_i takes α_i as its private key and $P_{pub_i} = \alpha_i P$ as the public key for vehicle $v_i \in V$, $1 \le i \le n$.

RV-ENCRP. This algorithm is completed by the region representative. We choose a random $f \in \mathbb{Z}_q^*$ and set the ciphertext for region information $m \in \{0,1\}^*$ to be $info_R = \left\langle fP, m \oplus H_2\left(g_R^f\right)\right\rangle$,where g_R is defined as $g_R = e(Q_R, P_{pub_{\mathcal{CS}}})$.

RV-MC. Given $info_R = \langle U, W\rangle$, any vehicle in the region that needs to participate in signing the encrypted region information $info_R$ computes $\sigma_i = \alpha_i H(W)$ with its own private key α_i. σ_i will be sent to the region representative. Let $R = \{v_{i_1}, ..., v_{i_r}\} \subseteq V$ be vehicles in the region that are going to contribute to the signing of the region information. By collecting all the σ_j for $j \in J = \{i_1, ..., i_r\}$, the region representative computes the multi-signature $\sigma = \sum_{j\in J} \sigma_j$. The region representative will then output $(info_R, R, \sigma)$ to the cloud server.

RV-Ver. Given $T = (info_R, R_{ID}, \sigma)$ and the list of public keys of the vehicles in R, $P_{pub_j} = \alpha_j P$, $j \in J = \{i_1, ..., i_r\}$, the cloud server computes $P_{pub_R} = \sum_{j\in J} P_{pub_j} = \sum_{j\in J} \alpha_j P$ and verifies $e(P, \sigma) = e(P_{pub_R}, H(W))$. If the equation holds, it output "1"; otherwise, it outputs "0".

RV-DECRP. If the output of the RV-Ver algorithm is "1", given $info_R = \langle U, W\rangle$, to obtain the encrypted message m, the cloud server will compute $W \oplus H_2(e(S_R, U))$.

The correctness of the equation in algorithm **RV-Ver** is elaborated as follows:

$$e(P, \sigma) = e\left(P, \sum\nolimits_{j\in J} \alpha_j H(W)\right) = e(P_{pub_R}, H(W))$$

The cloud can obtain the uploaded information through the acquired message $info_R = \langle U, W\rangle = \left\langle fP, m \oplus H\left(g_R^f\right)\right\rangle$. This can be demonstrated by the following formula. The initial encrypted region information is eventually acquired by the cloud through these calculations.

$$W \oplus H_2(e(S_R, U)) = m \oplus H_2\left(g_R^f\right) \oplus H_2(e(S_R, U)) = m$$

The main difference between the proposed information upload scheme and the signature method presented by Boldyreva *et al.* [33] is that the two roles of the sign collector and the verifier are separated in our scheme. The region representative needs to multiply the given signatures together and upload the message to the cloud. The cloud will continue the verification process according to the verification algorithm above. The other difference is that with the given information, the cloud can obtain the encrypted region information that has been signed by the vehicles.

VI. Analysis of our Proposed CATE Scheme

In this section, some analysis for CATE will be presented, including security analysis and a performance evaluation.

A. Security Analysis

OMU-CMA Security. Formally, the OMU-CMA security of the CATE scheme is guaranteed by the following theorem for preventing an adversarial cloud server from forging a vehicle's signature.

Theorem 1: If there exists a polynomial-time adversarial cloud server $\mathcal{A}$ that can break the OMU-CMA security of the CATE scheme with advantage $\mathrm{Adv}_{\mathcal{TLC},\mathcal{A}}^{\mathrm{OMU-CMA}}$, then there exists a polynomial-time adversary $\mathcal{B}$ that can break the one-more-unforgeability security of the underlying signature scheme BLS with advantage at least $\mathrm{Adv}_{\mathcal{BLS},\mathcal{B}}^{\mathrm{OMU}} \ge \mathrm{Adv}_{\mathcal{TLC},\mathcal{A}}^{\mathrm{OMU-CMA}}$.

Proof. We construct the algorithm $\mathcal{B}$ to prove the theorem, which invokes an adversarial cloud server $\mathcal{A}$ to break the *one-more-unforgeability* security of the BLS scheme in the following manner.

In the Setup stage, $\mathcal{B}$ receives the public key P_{pk} from the signing oracle and sends P_{pk} to $\mathcal{A}$. In the MC-Query stage, upon receiving a queried TL value τ, $\mathcal{B}$ queries τ to the signing oracle to obtain the signature x and returns the hash value of the returned signature as $\gamma = xH(\tau)$ to $\mathcal{A}$. In the Ver stage, if $\mathcal{A}$ outputs $q_k + 1$ valid TL/confirmed-TL pairs $\{(\tau_i, \gamma_i)\}_{1\le i\le q_k+1}$, where q_k is the query number, then, for each i, $\mathcal{B}$ looks up τ_i in the hash query record for the corresponding signature x_i and outputs $\{(\tau_i, x_i)\}_{1\le i\le q_{k+1}}$ as the $q_k + 1$ valid message/signature pairs as its forgery signatures. Otherwise, $\mathcal{B}$ aborts.

Note here that the above $\mathcal{B}$ is indistinguishable from the original OMU-CMA game from the perspective of the adversary $\mathcal{A}$; therefore, $\mathcal{A}$ can successfully output

$q_k + 1$ valid TL/confirmed-TL pairs with the advantage $\mathrm{Adv}_{\mathcal{TLC},\mathcal{A}}^{\mathrm{OMU-CMA}}(\lambda)$, which means that $\mathcal{B}$ can break the one-more-unforgeability security of BLS with advantage at least $\mathrm{Adv}_{\mathcal{BLS},\mathcal{B}}^{\mathrm{OMU}} \geq \mathrm{Adv}_{\mathcal{TLC},\mathcal{A}}^{\mathrm{OMU-CMA}}$. □

AEF-CMA Security. Here, we discuss the AEF-CMA security of the CATE scheme. The concept is guaranteed by the following theorem for preventing an adversarial region representative from forging one of the vehicles' signatures.

Boneh *et al.* [34] proved that the GS signature scheme is secure against existential forgery under chosen message attack in the random oracle model assuming that the underlying group is GDH.

Here, we discuss the AEF-CMA security of the region information upload method **RV-MS** of our CATE scheme. This concept allows the adversary to corrupt all the participants except for one vehicle, the only honest vehicle. We have the following theorem.

Theorem 2: Let $\mathbb{G}_1$ be a GDH group. Then, **RV-MS** is AEF-CMA secure in the random oracle model. If there exits a polynomial-time adversary $\mathcal{A}$ that can break the AEF-CMA security of the above method RV-MS with advantage $\mathrm{Adv}_{\mathcal{RV},\mathcal{A}}^{\mathrm{AEF-CMA}}(\lambda)$, then there exists a polynomial-time adversary $\mathcal{B}$ that can break the chosen message attack of the aforementioned GS scheme with advantage at least $\mathrm{Adv}_{\mathcal{GS},\mathcal{B}}^{\mathrm{CMA}} \geq \mathrm{Adv}_{\mathcal{RV},\mathcal{A}}^{\mathrm{AEF-CMA}}$.

Proof. The proof for the theorem can be intuitively described as follows. We construct an algorithm $\mathcal{B}$ that can derive a forgery of the previously unsigned message if $\mathcal{A}$ can frame an honest player by constructing a valid multi-signature on some message without intervention by this honest player.

In the Setup stage, $\mathcal{B}$ receives the public key P_{pub_1} and accesses the random hash oracle and the signing oracle, and it gives $\mathcal{A}$ the public key $pk_1 = P_{pub_1}$. $\mathcal{A}$ possesses $r-1$ pairs of public and secret keys $(\alpha_2, P_{pub_2}), ..., (\alpha_r, P_{pub_r})$. In the MC-Query stage, upon receiving a queried message m, $\mathcal{B}$ queries m to the signing oracle to obtain the signature σ_m and returns it to $\mathcal{A}$. In the Output stage, if $\mathcal{A}$ asks the honest player to participate in the multi-signature generation protocol on some message $info_R$, $\mathcal{B}$ forwards the query to its signing oracle and returns the reply back to $\mathcal{A}$. At some point, $\mathcal{A}$ outputs an attempted forgery $T = (info_R, R, \sigma_R)$. $\mathcal{B}$ computes $\sigma{=}\sigma_R \cdot \sum_{j \in J/\{1\}} \left(H(info_R)^{-\alpha_j}\right)$ and outputs $(info_R, \sigma)$.

Clearly, $\mathcal{B}$ succeeds in the forgery in this game whenever $\mathcal{A}$ is successful; in other words, $\mathcal{B}$ can break the chosen message attack of the aforementioned GS scheme with advantage at least $\mathrm{Adv}_{\mathcal{GS},\mathcal{B}}^{\mathrm{CMA}} \geq \mathrm{Adv}_{\mathcal{RV},\mathcal{A}}^{\mathrm{AEF-CMA}}$. □

IND-RID-CMA Security. IBE was proven to be secure in [34]. IND-RID-CMA security ensures that no other entity outside of the region can learn any information about the region. The following theorem is presented.

Theorem 3: Suppose that there exits a polynomial-time adversary $\mathcal{A}$ that can break the IND-RID-CMA security of the above CATE scheme with advantage $\mathrm{Adv}_{\mathcal{RV},\mathcal{A}}^{\mathrm{IND-RID-CMA}}$. Then, there exists a polynomial-time adversary $\mathcal{B}$ that can break the chosen plaintext security of the underlying IBE signature scheme with advantage at least $\mathrm{Adv}_{\mathcal{IBE},\mathcal{B}}^{\mathrm{IND-ID-CPA}} \geq 1/q_k \cdot \mathrm{Adv}_{\mathcal{RV},\mathcal{A}}^{\mathrm{IND-RID-CMA}}$, where q_k is the number of queries.

Proof. Algorithm $\mathcal{B}$, which simulates the challenger in the IND-ID-CPA model to play the game with $\mathcal{A}$, is constructed to prove the theorem. The goal of $\mathcal{B}$ is to break the chosen plaintext security of the scheme IBE. Given the public key $P_{pub_{\mathcal{CS}}}$ of IBE, $\mathcal{B}$ interacts with $\mathcal{A}$ as follows.

In the Setup stage, $\mathcal{B}$ runs the RV-KeyGen$_{\mathcal{CS}}$ algorithm to generate the key pair $(P_{pub_{\mathcal{CS}}}, \beta_{\mathcal{CS}})$ and gives $P_{pub_{\mathcal{CS}}}$ to the adversary $\mathcal{A}$. In the Query-I stage, when $\mathcal{A}$ queries the ciphertext $info_R$ for the region information m in region R_{ID}, $\mathcal{B}$ first accesses the random oracle H for $H(R_{ID})$. $\mathcal{B}$ then generates the ciphertext $info_R$ and returns the result to $\mathcal{A}$. In the Challenge stage, upon receiving two challenge region informations m_0 and m_1 from $\mathcal{A}$, instead of querying m_b to the encryption algorithm for $info_{R_b}$, $\mathcal{B}$ simply picks f randomly and generates the challenge ciphertext $info_{R_q}$ of m_b. $\mathcal{B}$ then sends it to $\mathcal{A}$. In the Query-II stage, $\mathcal{B}$ simulates in the same way as described in Query-I stage. In the Output stage, after $\mathcal{A}$ outputs its guess b' on b, $\mathcal{B}$ picks an input element from the ENCRP algorithm and outputs it as its $info_R$.

If $\mathcal{A}$ never queries $(m_b, info_{R_b})$, $= \Pr[b = b'] = 1/2$. Therefore, $\Pr[b = b'] = \mathrm{Adv}_{\mathcal{RV},\mathcal{A}}^{\mathrm{IND-RID-CMA}}$ when $\mathcal{A}$ queries $(m_b, info_{R_b})$. Thus, $\mathcal{B}$ can forge the ciphertext with advantage $\mathrm{Adv}_{\mathcal{IBE},\mathcal{B}}^{\mathrm{IND-ID-CPA}} \geq 1/q_k \cdot \mathrm{Adv}_{\mathcal{RV},\mathcal{A}}^{\mathrm{IND-RID-CMA}}$. □

Based on the above-mentioned theorems, we make the following comment.

Theorem 4: The CATE scheme is secure if the BLS short signature, GS multi-signature and IBE encryption schemes are secure.

Proof. The conclusion can be drawn from the aforementioned ***Theorem*** 1, ***Theorem*** 2, and ***Theorem*** 3 that this theorem can be proven. □

The security analysis indicates that our protocol can resist a variety of common threats, such as man-in-the-middle attack, replay attack, etc. In order to well present the security properties of our protocol, the proposed CATE is compared with SPECS [22] in terms of message integrity and authentication, privacy preserving, replay attack resistance, eavesdropping resistance, physical attack resistance, man-in-the-middle attack resistance, de-synchronization attack resistance and forward security. The comparison results are listed in Table. II. From Table. II, we can see that CATE is more secure than SPECS.

B. Performance Evaluation

In this subsection, we will introduce the performance evaluation of CATE and compare it with state-of-the-art research using numerical results. It is worth noting that, in our simulation, the access rules of all regions are the same, which does not affect our analysis of the security and efficiency of the proposed scheme. Besides, the speed of vehicles in cities is limited. Note that, overspeed vehicles are not considered in our scheme. In our simulation, the maximum speed of the vehicle is set to be 60km/h.

TABLE II: Security comparison between CATE and SPECS

Security properties	**SPECS**	**CATE**
Message Integrity and Authentication	√ [1]	√
Privacy Preserving	√	√
Replay Attack Resistance	√	√
Eavesdropping Resistance	× [2]	√
Physical Attack Resistance	√	√
Man-In-The-Middle Attack Resistance	√	√
De-Synchronization Attack Resistance	√	√
Forward Security	×	√

[1] √ denotes that the scheme satisfies the security property.
[2] × denotes that the scheme does not satisfy the security property.

1) Computation Overhead: The newcomer-representative authentication and the trustworthiness level confirmation parts are all auxiliary functions for making the scheme more secure and trustworthy.

The trustworthiness level confirmation part is utilized to ensure that the TL value provided by the cloud is acceptable to the vehicle's user. The analysis of this part is as follows: **TLC-KeyGen** costs 1 scalar multiplication in $\mathbb{G}_1$, **TLC-Conf** costs 1 hash operation and 1 scalar multiplication in $\mathbb{G}_1$, and **TLC-Ver** costs 2 pairing computations.

The most significant part is the joint information certification part. In this part, all members in a region participate in a multi-signature operation and help encrypt the uploaded information.

According to the definition of the RV-IU method of the CATE scheme, the computational costs of the phases in the RV-IU method are listed as follows. If there are n vehicles in the network, **RV-KeyGen**$_{CS}$ costs 2 scalar multiplications in $\mathbb{G}_1$ and 1 MapToPoint hash operation. **RV-KeyGen** costs n scalar multiplications in $\mathbb{G}_1$. **RV-ENCRP** costs 1 hash operation, 1 scalar multiplication in $\mathbb{G}_1$, 1 XOR operation, 1 pairing computation and 1 group exponentiation in $\mathbb{G}_2$. If there are $r \leq n$ members in the region, **RV-MC** costs r hash operation, r scalar multiplications in $\mathbb{G}_1$ and (r-1) additions in $\mathbb{G}_1$. **RV-Ver** costs (r-1) additions in $\mathbb{G}_1$, 1 MapToPoint hash operation and 2 pairing computations. **RV-DECRP** costs 1 hash operation, 1 XOR operation and 1 pairing computation.

The computational cost analysis of the joint information certification part in terms of different roles in the RV-IU method is given in Table III, compared with the SPECS scheme presented in [22].

In Table III, M represents a scalar multiplication, H indicates a MapToPoint hash operation, XOR denotes an exclusive-OR operation, H_2 implies a hash function, A represents an addition operation, P indicates a pairing computation, E represents an exponentiation computation, and C denotes a concatenation operation. Each vehicle in the region costs 2M+1H for signing the message. The region representative of a region with r members in the region costs $1H_2$+1M+1XOR+1P+1E+$(r-1)$A for encrypting messages and adding the signs of vehicles. Table III implies that the performance of our scheme is better than that of SPECS when there is one vehicle in the region. The advantage of our scheme will be more obvious when the number of vehicles increases in the region, since the proposed CATE scheme utilizes a multi-signature process to sign files, whereas SPECS uses a BLS scheme. In addition, the encryption operation of CATE is only operated by the RR. Therefore, a region with many vehicles only needs to perform the region information encryption one time.

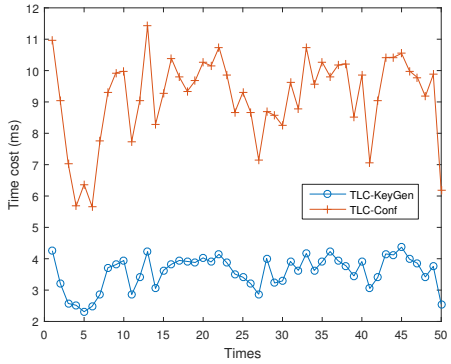

Fig. 6: Computation time cost in the TLC method of CATE

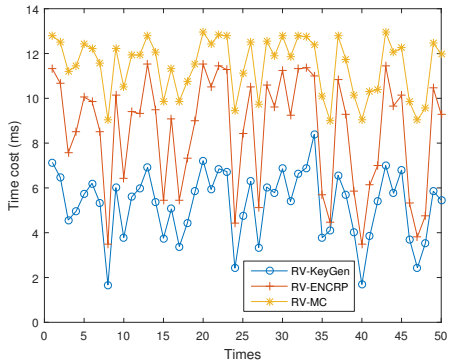

Fig. 7: Computation time cost in the RV-IU method of CATE

2) Simulation Results: To evaluate the efficiency of the proposed scheme, we implement the scheme with the GNU Multiple Precision Arithmetic (GMP) library and Pairing-Based Cryptography (PBC) library [1]. The experiment utilizes the C language on a Linux system with Ubuntu 16.04 TLS, a 2.60 GHz Intel(R) Xeon(R) CPU E5-2650 v2, and 8 GB of RAM.

We first simulate each phase implemented by the vehicles and region representative of the CATE scheme. There is no computational cost of the cloud sever for the clients. Therefore, we do not consider the time cost of the cloud.

Fig. 6 shows the time cost of two phases in the trustworthiness level confirmation. The confirmation phase is a signature process and requires the highest computation time from a vehicle. Fig. 7 demonstrates the **RV-KeyGen**, **RV-ENCRP** and **RV-MC** algorithms in the RV-IU method of the joint information certification process. The time cost of **RV-MC**, which is executed by both the vehicle and the region representative, is the largest. The cost of a vehicle is

[1] https://crypto.stanford.edu/pbc/

TABLE III: Computational Comparisons between CATE and SPECS

	One vehicle in the region	r **vehicles in the region**	**Vehicle authentication**	**Trustworthiness evaluation**
Our Scheme	1H+1H_2+3M+1XOR+1P+1E+1A	rH+1H_2+(1+2r)M+1XOR+1P+1E+$(r-1)$A	Yes	Yes
SPECS	2H+1H_2+6M+1XOR+1A+1C	2rH+$r$$H_2$+6$r$M+$r$XOR+$r$A+$r$C	Yes	No

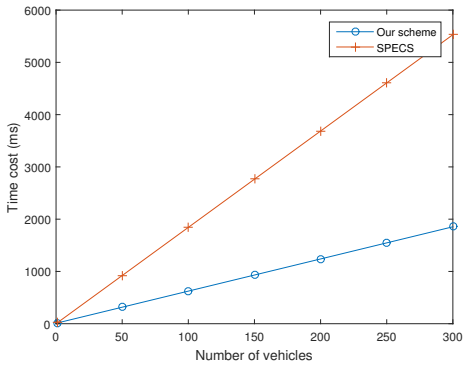

Fig. 8: Computation time cost comparison

acceptable. Note that the x-axis label for Fig. 6 and 7 implies the simulation times in the PBC. From these curves, we can see that computational cost of each algorithm in different methods fluctuates within a certain range. These curves show that the computational cost of the same algorithm may change under different simulation times. The uploading phase of the proposed CATE scheme is first simulated and compared with a similar phase of the SPECS scheme.

Fig. 8 illustrates the comparison of the time cost between the CATE and SPECS schemes. To better reflect the performance comparison in Fig. 8, the average value of the computational cost under 50 simulation times is used. The time cost of data uploading implemented by the vehicles and the region representative under the CATE scheme is compared with the message signing phase implemented by the vehicle and RSU under the SPECS scheme. The time cost of the CATE scheme is lower than that of the SPECS scheme. This is because the proposed CATE scheme utilizes a multi-signature process to sign files, whereas SPECS uses a BLS scheme. In addition, the encryption operation of CATE is achieved by the region representative. Therefore, a region only needs to encrypt region information one time.

VII. Conclusion

In this paper, we proposed a novel trustworthiness evaluation system for securely and fairly evaluating each vehicle in a network. Supported by the novel system, we proposed a cloud-aided trustworthiness evaluation scheme for incompletely predictable vehicular ad hoc networks. The scheme can provide newcomer-representative authentication, trustworthiness level confirmation and joint information certification. The analysis shows that the proposed scheme is suitable for vehicles in incompletely predictable networks and can provide vehicle privacy protection. In our future work, the integrity of the uploaded region information will be verified.

Acknowledgment

This work is supported by the National Natural Science Foundation of China under Grant No. 61672295, No. U1836115, the State Key Laboratory of Cryptology under Grant No. MMKFKT201830, the CICAEET fund, and the PAPD fund.

References

[1] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," *Journal of Network & Computer Applications*, vol. 76, pp. 37–48, 2016.

[2] T. Zhou, S. Jian, L. Xiong, W. Chen, and H. Tan, "Logarithmic encryption scheme for cyberphysical systems employing fibonacci Q-matrix," *Future Generation Computer Systems*, 2018, DOI: 10.1016/j.future.2018.04.008.

[3] J. Shen, C. Wang, A. Wang, X. Sun, S. Moh, and P. C. Hung, "Organized topology based routing protocol in incompletely predictable ad-hoc networks," *Computer Communications*, 2016.

[4] A. Castiglione, A. D. Santis, B. Masucci, and F. Palmieri, "Cryptographic hierarchical access control for dynamic structures," *IEEE Transactions on Information Forensics & Security*, vol. 11, no. 10, pp. 2349–2364, 2016.

[5] J. Liu, J. Ma, W. Wu, X. Chen, X. Huang, and L. Xu, "Protecting mobile health records in cloud computing: A secure, efficient, and anonymous design," *Acm Transactions on Embedded Computing Systems*, vol. 16, no. 2, p. 57, 2017.

[6] X. Huang, X. Chen, J. Li, Y. Xiang, and L. Xu, "Further observations on smart-card-based password-authenticated key agreement in distributed systems," *IEEE Transactions on Parallel & Distributed Systems*, vol. 25, no. 7, pp. 1767–1775, 2014.

[7] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 10, pp. 2402–2415, 2017.

[8] C. Wang, J. Shen, C.-F. Lai, R. Huang, and F. Wei, "Neighborhood trustworthiness based vehicle-to-vehicle authentication scheme for vehicular ad hoc networks," *Concurrency and Computation: Practice and Experience*, 2018, DOI: 10.1002/cpe.4643.

[9] P. Li, J. Li, Z. Huang, T. Li, C. Z. Gao, S. M. Yiu, and K. Chen, "Multi-key privacy-preserving deep learning in cloud computing," *Future Generation Computer Systems*, vol. 74, no. C, pp. 76–85, 2017.

[10] T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation," *IEEE Transactions on Computers*, vol. 65, no. 8, pp. 2363–2373, 2016.

[11] Y. Ren, J. Shen, D. Liu, J. Wang, and J. U. Kim, "Evidential quality preserving of electronic record in cloud storage," *Journal of Internet Technology*, vol. 17, no. 6, pp. 1125–1132, 2017.

[12] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," *IEEE Transactions on Computers*, vol. 64, no. 2, pp. 425–437, 2015.

[13] C. Wang, W. Zheng, S. Ji, Q. Liu, and A. Wang, "Identity-based fast authentication scheme for smart mobile devices in body area networks," *Wireless Communications and Mobile Computing*, 2018, DOI: 10.1155/2018/4028196.

[14] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 616–629, 2011.

[15] Y. M. Chen and Y. C. Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs," *Journal of Communications & Networks*, vol. 15, no. 2, pp. 153–163, 2013.
[16] R. A. Shaikh and A. S. Alzahrani, "Intrusionaware trust model for vehicular ad hoc networks," *Security & Communication Networks*, vol. 7, no. 11, pp. 1652–1669, 2014.
[17] J. A. F. F. Dias, J. J. P. C. Rodrigues, X. Feng, and C. X. Mavromoustakis, "A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 12, pp. 7929–7937, 2015.
[18] C. A. Kerrache, C. T. Calafate, N. Lagraa, J. Cano, and P. Manzoni, "RITA: Riskaware trustbased architecture for collaborative multihop vehicular communications," *Security & Communication Networks*, vol. 9, no. 17, pp. 4428–4442, 2016.
[19] M. Raya, P. Papadimitratos, V. D. Gligor, and J. P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *proceedings of IEEE INFOCOM 2008. the Conference on Computer Communications*, 2008, pp. 1238–1246.
[20] S. Park, B. Aslam, and C. C. Zou, "Long-term reputation system for vehicular networking based on vehicle's daily commute routine," in *proceedings of IEEE Consumer Communications and Networking Conference*, 2011, pp. 436–441.
[21] J. Timpner, D. Schurmann, and L. Wolf, "Trustworthy parking communities: Helping your neighbor to find a space," *IEEE Transactions on Dependable & Secure Computing*, vol. 13, no. 1, pp. 120–132, 2016.
[22] S. J. Horng, S. F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, and M. K. Khan, "b-SPECS+: Batch verification for secure pseudonymous authentication in VANET," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1860–1875, 2013.
[23] J. a. G. Filho, A. Patel, B. L. A. Batista, and J. C. Júnior, "A systematic technical survey of DTN and VDTN routing protocols," *Computer Standards & Interfaces*, vol. 48, pp. 139–159, 2016.
[24] D. He, S. Zeadally, N. Kumar, and J. H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, 2016, doi: 10.1109/JSYST.2016.2544805.
[25] A. Shokrollahi and M. N. Maybodi, "An energy-efficient clustering algorithm using fuzzy c-means and genetic fuzzy system for wireless sensor network," *Journal of Circuits Systems & Computers*, vol. 26, no. 1, 2016.
[26] A. M. Dziekoski and R. O. Schoeneich, "DTN routing algorithm for networks with nodes social behavior," *International Journal of Computers Communications & Control*, vol. 11, no. 4, pp. 457–471, 2016.
[27] J. Shen, C. Wang, A. Wang, Q. Liu, and Y. Xiang, "Moving centroid based routing protocol for incompletely predictable cyber devices in cyber-physical-social distributed systems," *Future Generation Computer Systems*, 2017.
[28] M. Pouryazdan, B. Kantarci, T. Soyata, and H. Song, "Anchor-assisted and vote-based trustworthiness assurance in smart city crowdsensing," *IEEE Access*, vol. 4, pp. 529–541, 2016.
[29] J. Shen, H. Tan, S. Moh, and I. Chung, "Enhanced secure sensor association and key management in wireless body area networks," *Journal of Communications & Networks*, vol. 17, no. 5, pp. 453–462, 2015.
[30] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block design-based key agreement for group data sharing in cloud computing," *IEEE Transactions on Dependable & Secure Computing*, 2017, doi: 10.1109/TDSC.2017.2725953.
[31] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," *Journal of cryptology*, vol. 17, no. 4, pp. 297–319, 2004.
[32] X. Chen, F. Zhang, W. Susilo, H. Tian, J. Li, and K. Kim, "Identity-based chameleon hashing and signatures without key exposure," *Information Sciences*, vol. 265, no. 5, pp. 198–210, 2014.
[33] A. Boldyreva, "Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme," in *International Workshop on Public Key Cryptography*. Springer, 2003, pp. 31–46.
[34] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Annual International Cryptology Conference*. Springer, 2001, pp. 213–229.