sensors

MDPI

Article

Privacy-Preserving Smart Road-Pricing System with Trustworthiness Evaluation in VANETs †

Qingfeng Zhu [1], **Sai Ji** [2], **Jian Shen** [1,3,*] and **Yongjun Ren** [1]

1 School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China; 20191220041@nuist.edu.cn or q_f_zhu@126.com (Q.Z.); 002315@nuist.edu.cn (Y.R.)
2 Suqian University, Suqian 223800, China; jisai@nuist.edu.cn
3 The Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen 518000, China
* Correspondence: shenjian@nuist.edu.cn

† This manuscript is extension version of the conference paper: Zhu Q.; Ji S.; Liu Q. Privacy-Preserving Smart Road Pricing System in Smart Cities. In Proceedings of the 2021 IEEE Conference on Dependable and Secure Computing (DSC), Aizuwakamatsu, Fukushima, Japan, 30 January–2 February 2021.

Abstract: With the advanced development of the intelligent transportation system, vehicular ad hoc networks have been observed as an excellent technology for the development of intelligent traffic management in smart cities. Recently, researchers and industries have paid great attention to the smart road-tolling system. However, it is still a challenging task to ensure geographical location privacy of vehicles and prevent improper behavior of drivers at the same time. In this paper, a reliable road-tolling system with trustworthiness evaluation is proposed, which guarantees that vehicle location privacy is secure and prevents malicious vehicles from tolling violations at the same time. Vehicle route privacy information is encrypted and uploaded to nearby roadside units, which then forward it to the traffic control center for tolling. The traffic control center can compare data collected by roadside units and video surveillance cameras to analyze whether malicious vehicles have behaved incorrectly. Moreover, a trustworthiness evaluation is applied to comprehensively evaluate the multiple attributes of the vehicle to prevent improper behavior. Finally, security analysis and experimental simulation results show that the proposed scheme has better robustness compared with existing approaches.

Keywords: intelligent transportation system; road-tolling system; privacy preservation; tolling violations; trustworthiness evaluation

Citation: Zhu, Q.; Ji, S.; Shen, J.; Ren, Y. Privacy-Preserving Smart Road-Pricing System with Trustworthiness Evaluation in VANETs. *Sensors* **2021**, *21*, 3658. https://doi.org/10.3390/s21113658

Academic Editors: Lei Zhang, Weizhi Meng and Kaitai Liang

Received: 9 April 2021
Accepted: 18 May 2021
Published: 24 May 2021

1. Introduction

Vehicular ad hoc networks (VANETs) have attracted keen interest from researchers and industries [1–3]. VANETs have been studied in depth over recent years, which has contributed to the construction of smart traffic networks in smart cities. As a promising technology in Intelligent Transportation Systems, VANETs play a key role in avoiding traffic congestion, reducing accidents, decreasing fuel consumption, road safety, and driving comfort [4–6]. Optimal road-pricing algorithms force drivers to choose the best routes with less payment, which solves problems in modern society such as exhaust gas pollution.

Since many efforts have focused on developing new tolling methods to better meet the requirements of VANETs in smart cities, road-pricing has evolved into smarter ways, such as the smart road-pricing (SRP) system. Instead of depending on physical equipment, SRP can combine the Global Navigation Satellite System with electronic equipment in vehicles, which makes room for other vehicles and reduces road upkeep [3]. However, properties of decentralization, heterogeneity, and non-trustworthiness in VANETs pose significant challenges in securing message transmission. Therefore, security issues are a priority when deploying this kind of tolling approach, in that malicious vehicles may try to pay less or

evade payments. Moreover, the adversary may map the real location of vehicles with user identity to obtain privacy. Therefore, the location of vehicle disclosure may impose heavy threats to drivers.

The trustworthiness of a vehicle is another reference for guaranteeing reliable communication among vehicles or other infrastructure. In [7], a comprehensive evaluation system for vehicles is proposed for the evaluation of various attributes of vehicles. Such an evaluation scheme can provide a real-time update of vehicle status. Various types of communication in VANETs are referenced in [8–10]. Vehicles in smart cities can communicate with other vehicles, which is referred to as vehicle-to-vehicle (V2V) communication. Vehicles can also communicate with other infrastructure such as roadside units (RSUs) or the traffic control center (TCC), which is known as vehicle-to-infrastructure (V2I) communication [7]. Additionally, communication between infrastructure can be normal. The communication types in VANETs have been investigated and studied in depth. In our scheme, V2I communication provides a secure channel for vehicles to transmit their geolocation messages to nearby RSUs. At this point, the trustworthiness of vehicles transmitting messages needs to be assessed. Basically, the trustworthiness of a vehicle mainly comes from how many times it has violated tolling rules when using the toll road.

In this paper, an efficient and secure road-pricing system is proposed to better meet the requirements of smart cities. Our purpose is to protect vehicle location privacy during the process of driving while guaranteeing that no driver can perform a tolling violation. In our scheme, only the TCC can trace the real routes of vehicles to protect user privacy disclosure. Moreover, the trustworthiness evaluation of vehicles is applied. The higher the trusted value of a vehicle, the more convenient the services it can obtain, such as priority parking or cheap deals on fuel.

1.1. Motivation

The smart road-tolling system has drawn significant attention from researchers and industry, as it succeeds in relieving traffic pressure, reducing fuel consumption, and promoting the construction of eco-friendly cities. Though many smart road-pricing schemes have been proposed, they may not apply practically due to the large communication overhead and redundant operations. To cope with these issues, a privacy-preserving smart road-pricing scheme with trustworthiness evaluation is proposed. First, the term privacy means that a vehicle route needs to be kept secret during communication with RSUs or other vehicles, otherwise malicious entities may track it. Secondly, the identity of the vehicle itself should be protected.

Our contributions: In this paper, an efficient and secure road-pricing system with trustworthiness evaluation is proposed. The contributions of our proposed scheme are as follows:

- A novel effective road-tolling violation scheme is proposed. Smart road-tolling in smart cities can be a challenging task given that tolling violation happens frequently. In this paper, a novel road-tolling violation scheme is proposed. The proposal combines video surveillance cameras (VSCs) and RSUs to detect malicious behavior for a vehicle even if a driver turns off his/her on-board unit (OBU) completely from its vehicle. To be certain, the TCC compares the data collected by VSCs, which are fixed on the pivotal toll road, with the routes collected by RSUs to check whether they are the same.
- A scalable trustworthiness evaluation of the vehicle scheme is investigated. The trustworthiness of a vehicle shows the act of passing through toll roads in the past. In this paper, we present a novel scalable trustworthiness evaluation of vehicle scheme to handle the behaviors of sending false geolocation messages or malicious vehicle users, such as the impersonation of another legitimate vehicle. Therefore, to behave truthfully is the best choice for drivers when using toll roads. The higher the trusted value of a vehicle, the better the access to infrastructure services such as priority parking.
- The detection rate of toll evasion with high efficiency is achieved. On the one hand, though many theoretic smart road-tolling schemes have been proposed, they suffer

from a lot of computational overheads. On the other hand, these proposed schemes cannot record tolling violations effectively. That is to say, the schemes which have already been proposed are inefficient. In our scheme, PUF-based VSCs are fixed to pivotal places that can monitor the of passing vehicles accurately. Therefore, the detection rate of toll evasion in our proposed scheme is higher compared to others.

1.2. Organization

The structure of this paper is as follows: Section 2 presents related works. Section 3 describes the preliminaries that will be used later. Section 4 provides the system model of our proposed scheme and the design objections. Section 5 introduces a detailed description of our scheme, followed by security analysis in Section 6. Section 7 presents the performance of our scheme and a conclusion is provided after that.

2. Related Works

Privacy issues, especially vehicle geolocation data disclosure in road-pricing systems, have drawn widespread attention from researchers over recent years. Numerous solutions have been proposed to achieve security requirements in smart road-pricing.

Vehicle geolocation data can be collected by the OBU and the TCC easily. The encrypted geolocation data is then stored at the TCC, which can reduce the burden of OBU tremendously. Moreover, the TCC can respond in a timely manner when something urgent happens using to the data stored in it [3]. However, such a solution raises another threat after payment information finishes. Chen et al. [11] claimed that this information can be cracked by an external malicious attacker. Therefore, post hoc analysis concerning user traceability based on a user toll payment information scheme has been proposed by them. To avoid violating the location privacy of drivers, Popa et al. [12] proposed a scheme that can be applied to various location-based applications. The authors developed a practical protocol to compute the routing function concerning various tolling, the speed of vehicles, and delay estimation without revealing vehicle geolocation. To ensure the users always pay right tolls, homomorphic commitment [13] has been applied. Random spot-checks with cameras hidden on vehicles are employed to prevent dishonest drivers from cheating on their location. However, an anonymous network is needed to communicate their sensitive traveling data, which imposes heavy overheads on the system. More recently, a group signature [14] toll-pricing system has been proposed by Chen et al. [15] to achieve a balance between vehicle anonymity, computation, and communication overheads. In the proposed scheme, a high-efficiency group signature is deployed to sign each vehicle location before sending them to toll servers. Those vehicles are also grouped by a trusted authority according to criteria such as speed, reputation, and similarity, as per [3,16]. Vehicle privacy in this way can be better protected if proper group management is designed.

With the improvement of smart cities, the location privacy of vehicles plays a significant role in deploying smart electronic systems in VANETs. In 2016, a low-emission zone (LEZ) privacy-preserving road-tolling system was proposed in [17]. The authors divided LEZ into multiple zones, charging various prices according to the topology of the city and the level of congestion. However, the authors in [3] pointed out that vehicles need to authenticate themselves when entering or leaving a zone, which imposes heavy computational overheads. Therefore, a distributed, reliable, and secure pricing system was proposed by Siham Bouchelaghem et al. [3] to better meet the requirements of privacy preservation in SRP. The authors apply a threshold-based control system to discover malicious vehicles who try to cheat on their tolls. Once the accused drivers are tested, a toll server can take relevant measures to punish them. Moreover, the scheme can resist a variety of potential attacks, and the computation and communication overheads are considerably better behaved.

Location-based privacy for vehicles has been investigated actively in recent years. Reza Shokri et al. proposed a *k*-anonymity location privacy preservation scheme [18] in which the real locations of drivers are obfuscated by the construction of cloaking regions.

However, Fifi Farouk et al. [6] claimed that this scheme cannot be applied to low-density zones where the users who want to send requests must wait for k other users, which may lead to delays and degrade the quality of service. Levente Buttyan et al. [19] proposed that vehicles blind their real identities, which changes with some frequency to solve the problem of privacy disclosure. However, this method may be impractical when applied to long-term communication, because changing frequently may interrupt the quality of correspondence. Recently, Fifi Farouk et al. [6] proposed a location-based service (LBS) to protect the privacy of vehicles using fully homomorphic encryption [20] over advanced encryption standard [21]. However, they do not take road-tolling into consideration.

3. Preliminaries

In this section, we present the relative cryptographic primitives used in our scheme.

3.1. The Computational Diffie–Hellman (CDH) Assumption

The CDH problem used in our scheme is briefly defined in the following definition. Given an instance (P, aP, bP) where $a, b \in Z_p^*$, the computational Diffie–Hellman problem (CDH Problem) in a multiplicative group G is to compute abP. The success probability of any probabilistic, polynomial-time, 0/1-valued algorithm $\mathcal{A}$ to solve CDH problem in G can be defined as:

$$Suc_{\mathcal{A},G}^{CDH} = \mathrm{P}rob[\mathcal{A}(P, aP, bP) = 1 : a, b \in {}_R Z_q^*].$$

The CDH assumption is that for every adversary $\mathcal{A}$ in probabilistic polynomial time, the probability of $Suc_{\mathcal{A},G}^{CDH}$ is negligible.

3.2. Fuzzy Comprehensive Strategy (FCS)

Driver behavior cannot be determined by a single evaluation accurately, because of the uncertainty and complexity of their actions. Therefore, the fuzzy comprehensive strategy is used to evaluate the trustworthiness of drivers. With such a strategy, multiple attributes and actions are taken into consideration.

3.2.1. Vehicle Behavior Attributes

The behavior attributes of vehicles can be described by a variety of factors, including mileage, timings of vehicle accident records, maximum speed, number of passing tolling spots, and number of toll violations. The trustworthiness of vehicles can be evaluated by the attributes recorded in each vehicle OBU.

3.2.2. Entropy Method

Entropy was originally one of the parameters used to describe the state of matter in thermodynamics. It has been widely used to evaluate multiple-attribute comprehensive evaluation problems since it was introduced into information theory in 1948 by Shannon [22]. According to the degree of variation, information entropy can be used to calculate the entropy weight of attributes. Moreover, entropy weight can also be applied to correct the value to arrive at a more objective weight value.

3.2.3. Comprehensive Attribute Weight

Specifically, comprehensive attribute weight applies various important attributes to vehicle behavior. To obtain objective evaluation results, the attribute weight is not obtained from historical experience, but from the entropy weight mentioned previously. Considering the characteristics of each vehicle's multiple attributes, it is necessary to illustrate the attribute weight with a comprehensive method $W = \{w_1, w_2, \cdots, w_n\}$ where $\sum_{i=1}^{n} w_i = 1$.

3.3. Schnorr Signature

We apply the Schnorr signature [23] to realize our scheme. As with the Elgamal digital signature [24], the Schnorr digital signature is also based on the discrete logarithm problem. The Schnorr scheme minimizes the amount of message computation required to generate the signature. The main work of generating a signature is independent of the message and can be performed when the processor is idle. We chose two large primes p, q, where q is the prime factor of $p-1$ where p, q is assumed to be 1024, and a 160-bit integer respectively. $m \in Z_p$ is chosen randomly, and $m^q = 1 \bmod p$. The signature is $\delta_{Schnorr} = (r + s\mathrm{Y}) \bmod q$, where $\mathrm{Y} = H(M||m^r)$, s is the private key, $r \in Z_p$ and satisfies $0 < r < q$. The public key can be computed by $pk = m^{-s} \bmod p$. To verify the signature, the receiver computes $\xi = m^{\delta_{Schnorr}} pk^{H(M||m^r)} \bmod p$ and verifies whether $H(M||m^r) = H(M||\xi)$.

4. System and Design Objections

4.1. The System Model

The system model and design objections of this proposed scheme will be presented in this section. The system model is provided in Figure 1. Please note that for the convenience of display, we only give the model of part of the road for VANETs in Figure 1. In a real scenario, there would be multiple vehicles, RSUs, and VSCs.

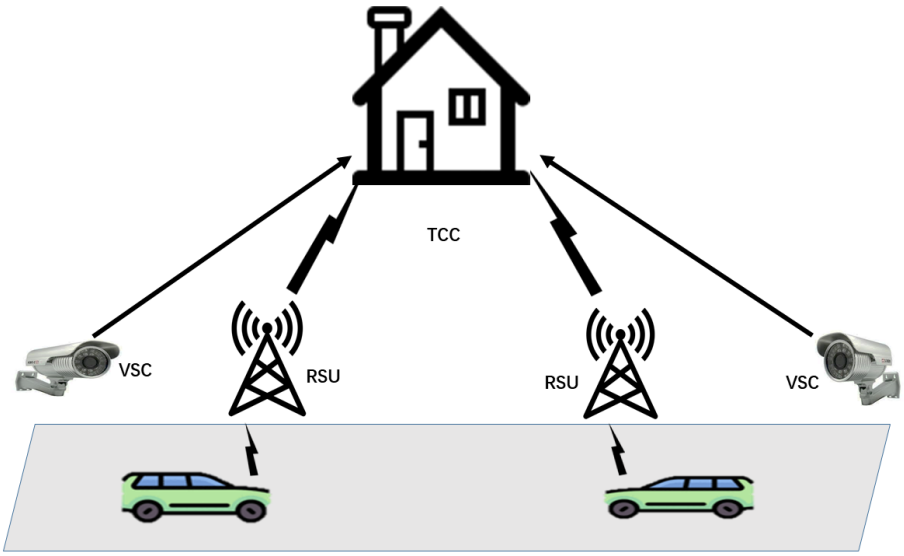

Figure 1. The system model for VANETs.

- TCC: In our proposed system, the TCC is a fully trusted entity that stores the real identities of vehicles, which are used to track the real driven routes of vehicles if necessary. It also acts as a judge to check whether a vehicle behaves incorrectly by comparing the data collected by VSCs with the data obtained by RSUs in its storage space. The TCC can be managed by a government organization and its computation and communication resources are powerful enough.
- Roadside Unit: As computing and communicating devices, RSUs can receive geolocation information transmitted from vehicles and then transfer them to a cloud server [4]. We assume that the RSUs in our scheme are trusted entities.
- Video Surveillance Camera: As common equipment in modern life, video surveillance cameras (VSCs) play a tremendous role in crime prevention, terrorist detection and obtaining evidence. Equipped with edge computing software units, VSCs have certain computing and storing capabilities. Installed in a pivotal place, the VSC can watch passing vehicles constantly [25]. To ensure security, we adopt the PUF-based VSCs that have been mentioned in [26] for the purpose of resisting various kinds of attacks. Moreover, when regulated by TCC, VSCs behave correctly and are never compromised.

- Vehicle: Equipped with an on-board unit (OBU), vehicles can realize communication and information exchange through a dedicated short-range communication (DSRC) protocol as proposed in [1,2,6,10,27,28]. The vehicle-to-vehicle and vehicle-to-RSU communications are wireless. In our proposed scheme, the vehicles may turn off their OBUs or impersonate a legitimate one to pay less.

4.2. The Threat Model

In this part, the threat model of the proposed scheme is presented in detail as follows:

A. An attacker can intercept messages transmitted between VSCs and the TCC, and then may alter, temper, or replay these messages.
B. A malicious vehicle may impersonate another legitimate one to send false geolocation messages for less payment when using toll roads.
C. An adversary may turn off his/her OBU to prevent nearby RSUs from detecting their driving signal to avoid payments.

4.3. The Design Goals

Security and privacy issues in VANETs are significant for mutual communication of entities. In this part, detailed design goals are presented as follows:

- Identity privacy preservation: Other malicious vehicles are not able to recover the vehicle's true identity.
- Message authentication: The TCC can check the validation of messages sent by VSCs, and messages sent by vehicles can also be checked by nearby RSUs.
- Conditional privacy preservation: In the event of a disagreement, the TCC can recover real identities of vehicles by analyzing messages sent by itself. To be specific, a malicious vehicle sends false geolocation message when it uses toll roads to reduce payment.
- Resistance of various kinds of attacks: Our proposed scheme can withstand some frequent attacks such as impersonation attack, modification attack, and man-in-the-middle attack, all of which are harmful to the normal execution of VANETs.

5. The Proposed Scheme

In this section, detailed descriptions of our privacy-preserving smart pricing scheme will be presented. The notations used in our scheme is presented in Table 1. Basically speaking, our scheme consists of five stages, named system bootstrapping, VSCs, vehicles and RSUs registration, geolocation message transmission, verification and comparison, trustworthiness evaluation process, and tolling bill.

5.1. System Bootstrapping

In this section, the TCC generates the system public parameters. The following operations are carried out by the TCC in our scheme:

- Choosing two large prime numbers p, q and an elliptic curve E which is defined by an equation $y^2 = x^3 + ax + b \bmod p$, where $a, b \in F_p$.
- A generator P is selected in the group G which with order q. The group G consists of all points on the elliptic curve and the infinity point O.
- $S \in {Z_q}^*$ will be selected randomly by the TCC as the system's private key, and the public key of the system can be therefore computed as $P_{pub} = S \cdot P$.
- Three secure collusion-resistance hash functions are chosen as $H_1 : G \rightarrow Z_q$, $H_2 : \{0,1\}^* \rightarrow Z_q$, $H_3 : \{0,1\}^* \times \{0,1\}^* \times G \times \{0,1\}^* \rightarrow Z_q$.
- TCC publicizes the public system parameters $\{p, q, a, b, P, P_{pub}, H_1, H_2, H_3\}$.

Table 1. Notations in our scheme.

Symbol	Description
G	An additive group with order q
E	An elliptic curve $y^2 = x^3 + ax + b \bmod p$
p, q	Represent two large prime numbers
S	The master key generated by traffic control center
P	The group generator
P_{pub}	The system public key, where $P_{pub} = S \cdot P$
AID_{vsc_i}	The pseudonym of VSC including $(AID_{vsc_i}{}^1, AID_{vsc_i}{}^2)$
$SK^i{}_{vsc}$	The private key of the VSC
$SK^i{}_v$	The private key of the vehicle
$RID^i{}_V$	The i-th true identity of the vehicle
$PID^i{}_V$	The i-th pseudonym identity of the vehicle
$RID^i{}_{VSC}$	The true identity of a VSC
$PID^i{}_{VSC}$	The i-th pseudonym identity of a VSC
$E_K()/D_K()$	The symmetric encryption/decryption function
H_1	Hash function $H_1 : G \rightarrow Z_q$
H_2	Hash function $H_2 : \{0,1\}^* \rightarrow Z_q$
H_3	Hash function $H_3 : \{0,1\}^* \times \{0,1\}^* \times G \times \{0,1\}^* \rightarrow Z_q$
n	The total number of vehicles passing a toll road in a period time
$\oplus$	Represent the exclusive-OR-operation
$\|\|$	The information concatenation operation

5.2. Entity Enrollment

Each PUF-based VSC must preload the system public parameters and register with the TCC, and then the TCC will assign $\{ID^i{}_{vsc}, S\}$ to each VSC over a secure channel. Each VSC checks whether the identities are equal to the stored ones. A denial request will be issued if one of them is not equal. Then, each VSC chooses a random number $x_i \in Z_q{}^*$ and computes the pseudonym of VSC which consists of two parts $AID_{vsc_i} = (AID_{vsc_i}{}^1, AID_{vsc_i}{}^2)$. Later, computing the private key $SK^i{}_{vsc}$ of the VSC where $\psi_i = H_2(AID_{vsc_i}||T_i||L_i)$, L_i is the location of the VSC, T_i is the timestamp. The specific calculation process is shown in Algorithm 1 lines 1 to 4.

In the process of VSC enrollment, each vehicle is equipped with a tamper-proof device which is preloaded with system public parameters and information $\{RID^i{}_v, S\}$ transmitted from the TCC over a secure channel. Then, each vehicle chooses a random number $\hbar_i \in Z_q{}^*$, and computes $\overline{\hbar_i}$ and $PID^i{}_v$; the private key corresponding to the vehicle anonymity is $SK^i{}_v$, the public key is $PK^i{}_v = SK^i{}_v \cdot P$. At the same time, each vehicle computes $\Lambda^i{}_v = SK^i{}_v \cdot P_{pub}$. The specific calculation process is shown in Algorithm 1. The specific calculation process is shown in Algorithm 1 lines 5 to 8.

Each RSU sends the real identity RID_{RSU_i} to the TCC over a secure channel, then the TCC chooses a random number $\varepsilon_i \in Z_q{}^*$ and computes E_i, the private key of corresponding RSU is $SK^i{}_{RSU}$, where T_i is the timestamp. The public key is $PK^i{}_{RSU}$ and compute $\Lambda^i{}_{RSU} = SK^i{}_{RSU} \cdot P_{pub}$, then the TCC send the $\{RID_{RSU_i}, SK^i{}_{RSU}, PK^i{}_{RSU}, E_i, \Lambda^i{}_{RSU}\}$ to the corresponding RSU over a secure channel. The specific calculation process is shown in Algorithm 1 lines 9 to 12.

Algorithm 1 Entities Enrollment

Require: $\{ID^i_{vsc}, S\}$;
1: $\forall\ \lambda \in {Z_q}^*$, computing $AID_{vsc_i{}^1} = x_i \cdot P$, $AID_{vsc_i{}^2} = RID^i_{vsc} \oplus H_1(x_i \cdot S \cdot P)$;
2: $\psi_i = H_2(AID_{vsc_i}||T_i||L_i)$;
3: $SK^i_{vsc} = x_i + \psi_i \cdot S \bmod q$;
4: **End for**;
Require: $\{RID^i_v, S\}$;
5: $\forall\ \hbar_i \in {Z_q}^*$, computing $\overline{\hbar_i} = \hbar_i \cdot P$, $PID^i_v = RID^i_v \oplus H_1(S \cdot \overline{\hbar_i}||T_i)$;
6: Computing vehicle private key $SK^i_v = \hbar_i \cdot H_2(PID^i_v||\overline{\hbar_i}||T_i) + S(\mathrm{mod}q)$;
7: Computing vehicle public key $PK^i_v = SK^i_v \cdot P$;
8: **End for**;
Require: RID_{RSU_i};
9: $\forall\ \varepsilon_i \in {Z_q}^*$, computing $E_i = \varepsilon_i \cdot P$;
10: Computing RSUs private key $SK^i_{RSU} = \varepsilon_i \cdot H_2(RID_{RSU_i}||E_i||T_i) + S(\mathrm{mod}q)$;
11: Computing RSUs public key $PK^i_{RSU} = SK^i_{RSU} \cdot P$;
12: **End for**;

5.3. Geolocation Message Transmission

The geolocation message transmission phase can be divided into two parts, which are separately named VSC evidence generation and transmission, and vehicle route information dissemination, respectively.

In the process of VSC evidence generation and transmission, each VSC which is deployed in a fixed position takes pictures of passing vehicles to record their route information. This information is then transmitted to the TCC. The TCC stores the evidence information transmitted from the VSCs in the database, which is specially designed for storing evidence. The detailed operations are as follows: assuming that a vehicle enters a pricing road, the corresponding road VSC chooses a random number $\omega_i \in {Z_p}^*$, and computes $W_i = \omega_i \cdot P$, $\alpha_i = H_3(AID_{vsc_i}||T_i||L_i||W_i||LP_i)$, and generates the evidence signature $\sigma_i = SK^i_{vsc} + \alpha_i \cdot \omega_i \bmod q$, where AID_{vsc_i} is the ith anonymity identity of the VSC, L_i is the ith location information of the vehicle, LP_i is ith vehicle license plate, which is bound to the driver's real identity. Then, the VSC sends $\{\sigma_i, AID_{vsc_i}, T_i, L_i, W_i, LP_i\}$ to the TCC.

In the process of vehicle route information dissemination, each vehicle sends its geolocation information when entering a toll road. The detailed executions are as follows: for the purpose of privacy protection, each vehicle entering a toll road computes a communication session key with the nearby RSU based on its own private key and the identity of a nearby RSU, where the communication session key can be calculated as $CSK_{v_i}{}^{RSU_i} = SK^i_v \cdot H_2(RID_{TCC}||RID_{RSU_i}||E_i||S||T_i) \cdot E_i + \Lambda^i_v$, where RID_{RSU_i} is the ith real identity of RSU. Then, choose a number $z_i \in {Z_q}^*$ randomly, and compute $Z_i = z_i \cdot P$, $Sig_v{}^i = SK^i_v + z_i \cdot H_2(RID_{TCC}||RID_{RSU_i}||M)(\mathrm{mod}q)$, where $Sig_v{}^i$ means the message signature generated by the passing vehicles and $M = (L_i||T_i||PID^i_v)$ represents the message transmitted by a vehicle who enters a toll road at the nearby RSU. To ensure vehicle location privacy, symmetric encryption is adopted to blind the message $C = E_K(M||Sig_v{}^i)$. Then, the generated message $\{PID^i_v, C, T_i, Z_i, \overline{\hbar_i}\}$ is transmitted to the nearby RSU.

5.4. Verification and Comparison

Upon receiving the message, the RSU operates as Algorithm 2 only if T_i is in its valid period: computing the communication session key DK to decrypt the ciphertext C to obtain $M||Sig_v{}^i$. To verify the $Sig_v{}^i$, the RSU validates whether the equation is true. Based on the received message, RSUs only need to perform $RID^i_v = PID^i_v \oplus H_1(S \cdot \overline{\hbar_i}||T_i)$ to obtain the true identities of passing vehicles. When obtaining the true identities of passing vehicles, RSUs forward $\{RID^i_v, L_i, T_i\}$ to the TCC over a secure channel for further road-tolling. Later, the TCC verifies the signature to judge whether the messages have been altered by a malicious adversary.

Algorithm 2 Verification

Require: $\{PID^i{}_v, C, T_i, Z_i, \overline{\hbar_i}\}$;

1: Computing $DK = SK^i{}_{RSU} \cdot H_2(PID^i{}_v||RID_{TCC}||RID_{RSU_i}||Z_i||S||T_i) \cdot E_i + \Lambda^i{}_{RSU}$;
2: Decrypting $M||Sig_v{}^i = D_{DK}(C)$;
3: Verifying whether $SK^i{}_{RSU} \cdot Sig_v{}^i \cdot P = DK + Z_i \cdot SK^i{}_{RSU} \cdot H_2(RID_{TCC}||RID_{RSU_i}||T_i||M)$;
4: **End for**;

The TCC executed the following operations:

- Verification of a single message

Checking the freshness of the T_i, the TCC rejects the message if the T_i is not fresh. The TCC checks whether the equation $\sigma_i \cdot P = AID_{vsc_i{}^1} + \psi_i \cdot P_{pub} + \alpha_i \cdot W_i$ holds.

- Verification of multiple messages

To speed up verification, many related works have been proposed [29–33]. Therefore, to improve verified efficiency, the small exponent test technique [34,35] is applied. Within such technology, a vector consisting of small random integers can be used to quickly detect any modification in the process of batch verification. Upon receiving multiple messages from VSCs, the TCC verifies the correctness of those messages. First, it checks the freshness of T_i. Messages merely with the valid T_i can be accepted. Second, a vector $\Gamma = \{\tau_1, \tau_2, \cdots, \tau_n\}$ is chosen randomly, where τ_i is a small random integer. After that, the TCC verifies whether Equation (1) holds.

$$\left(\sum_{i=1}^{n} \tau_i \cdot \sigma_i\right) \cdot P = \sum_{i=1}^{n} (\tau_i \cdot AID_{vsc_i{}^1}) + \left(\sum_{i=1}^{n} (\tau_i \cdot \psi_i)\right) \cdot P_{pub} + \sum_{i=1}^{n} (\tau_i \cdot \alpha_i \cdot W_i) \quad (1)$$

The TCC rejects the messages if the above equation fails to pass verification; otherwise, the TCC accepts them. Then, the TCC stores the messages in a database 1. For these monitoring messages $\{\sigma_1, AID_{vsc_1}, T_1, L_1, W_1, LP_1\}$, $\{\sigma_2, AID_{vsc_2}, T_2, L_2, W_2, LP_2\}$, $\cdots$, $\{\sigma_n, AID_{vsc_n}, T_n, L_n, W_n, LP_n\}$ from VSCs, the TCC first perform XOR operations $RID_{vsc} = AID_{vsc_i{}^2} \oplus H_1(x_i \cdot S \cdot P)$ to obtain the real identities of each VSC. Afterwards, the TCC stores these monitoring messages $\{RID_{vsc_1}, T_1, L_1, LP_1\}$, $\{RID_{vsc_2}, T_2, L_2, LP_2\}$, $\cdots$, $\{RID_{vsc_n}, T_n, L_n, LP_n\}$ in database 2. Specifically, the license plate (LP) of each vehicle in database 1 corresponds to the real identities in database 2. We assume that the PUF-based VSCs can never be compromised, and the messages recorded by them can be trusted. Therefore, the messages transmitted from these VSCs which are fixed on pivotal toll roads can be seen as a reference. Then, the TCC compares whether L_i stored in database 1 and database 2 are equal using an efficient comparison algorithm in the same period T_i.

5.5. Trustworthiness Evaluation and Tolling Bill

5.5.1. Trustworthiness Evaluation

There are various methods to explore and analyze user behaviors, such as [36,37]. To evaluate the attributes of the vehicle more accurately, a fuzzy comprehensive strategy is adopted in our scheme to analyze each vehicle behavior comprehensively, assuming that the $A = \{a_1, a_2, \cdots, a_n\}$ are vehicle n-th attributes which can be seen as trustworthiness evaluation indexes. $A^0 = \{a_1{}^0, a_2{}^0, \cdots, a_n{}^0\}$ denotes the initial attribute weight of each vehicle, and $T^t = \{t_1, t_2, \cdots, t_l\}$ means the l instances in time t_i. The following matrix $\overline{\mathrm{A}}$ is adopted to demonstrate the behavioral attribute clearly.

$$\overline{\mathrm{A}} = \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{l1} & A_{l2} & \cdots & A_{ln} \end{bmatrix}$$

where A_{ij} denotes the attribute a_i in the j-th instance. The normalized matrix $\overline{\Lambda}$ can be obtained by processing the fuzzy matrix $\overline{\mathrm{A}}$ in the following equation.

$$\Lambda_{ij} = \begin{cases} \frac{A_{ij} - min\{A_{1j}, \cdots, A_{lj}\}}{max\{A_{1j}, \cdots, A_{lj}\} - min\{A_{1j}, \cdots, A_{lj}\}}, A_{ij} \in P^+; \\ \frac{max\{A_{1j}, \cdots, A_{lj}\}}{max\{A_{1j}, \cdots, A_{lj}\} - min\{A_{1j}, \cdots, A_{lj}\}}, A_{ij} \in P^-. \end{cases}$$

where the P^+ and P^- represents the positive and negative attributes, respectively.

$$\overline{\Lambda} = \begin{bmatrix} \Lambda_{11} & \Lambda_{12} & \cdots & \Lambda_{1n} \\ \Lambda_{21} & \Lambda_{22} & \cdots & \Lambda_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \Lambda_{l1} & \Lambda_{l2} & \cdots & \Lambda_{ln} \end{bmatrix}$$

As previously mentioned, the entropy method used to demonstrate the uncertainty of things has determined multi-attribute comprehensive evaluation problems in a high-efficiency way. Specifically, the higher uncertainty of the attribute means the higher its weight. According to the normalization of the matrix $\overline{\Lambda}$, the TCC calculates $\bar{\Gamma}_{ij} = \frac{A_{ij}}{\sum_{i=1}^{l} A_{ij}}$ $(i = (1, 2, \cdots, l), j = (1, 2, \cdots, n))$. For each attribute in $j = (1, 2, \cdots, n)$, entropy weight can be calculated by the TCC as

$$\bar{w}_j = \frac{1 - \bar{w}}{n - \sum_{j=1}^{n} \bar{w}} \quad j = (1, 2, \cdots n) \tag{2}$$

where $\bar{w} = -\frac{1}{\ln(l)} \sum_{i-1}^{l} \bar{\Gamma}_{ij} \ln(\bar{\Gamma}_{ij})$. Therefore, the vehicle's initial trustworthiness value can be represented as the following equation

$$IT^V = \sum_{j=1}^{n} \frac{\bar{w}_j}{n} \sum_{i=1}^{l} \Lambda_{ij}. \tag{3}$$

Please note that the V_{rwd} and V_{psh} are the reward and punishment thresholds used to encourage honest vehicle behavior. To be specific, once the initial trustworthiness value is more than V_{rwd}, more reward Q will be awarded. Otherwise, the initial value will be deducted correspondingly.

The new trusted value of a driver will be increased if the comparison results are equal. By contrast, the new trusted value will be decreased. The following equation can be used to represent the final trustworthiness value for a vehicle

$$NEW^{V_i}{}_{TV} = \begin{cases} \max\{0, IT^{V_i} - Q\}, & 0 \le IT^{V_i} \le V_{rwd} \\ IT^{V_i} \quad , & V_{rwd} \le Q \le V_{psh} \\ \min\{1, IT^{V_i} + Q\}, & V_{psh} < Q \le 1 \end{cases} \tag{4}$$

5.5.2. Toll Bill

The final toll bill will be generated based on the trusted value $NEW^{V_i}{}_{TV}$ at the end of pricing period and then be sent to the drivers who use the toll road. For each vehicle, the TCC calculates the fee $g(T_i{}^j, L_i{}^j)$ with the billing function, where j represents the vehicle

using the toll road for j times. The final total costs of the i-th vehicle can be represented by $Bill^i{}_v = \sum_{j=1}^{n} g(T_i{}^j, L_i{}^j, NEW^{V_i}{}_{TV}{}^j)$, where the vehicle trusted value $NEW^{V_i}{}_{TV}$ is incorporated. To guarantee the integrity and authenticity of the bill, the TCC encrypts the bill using the public key of a vehicle, and then signs it using the private key of the TCC. Detailed operations of the TCC are as follows: randomly chosen numbers $\lambda \in Z_q{}^*$, and (Φ_1, Φ_2) are computed where $\Phi_1 = \lambda \cdot P, \Phi_2 = \lambda \cdot PK^i{}_v$. Afterwards, $\Re = Bill^i{}_v \cdot X_{\Phi_2} \bmod p$ and $\eta = \lambda - P_{pub} \cdot \Re \bmod q$ are calculated where X_{Φ_2} means the horizontal axis of Φ_2. Finally, the TCC generates the bill's signature $\sigma_{Bill^i{}_v} = \langle \Re || \eta || \Phi_1 \rangle$. The detailed generation process of the toll bill is provided in Algorithm 3.

Algorithm 3 Generating Tolling Bill Signature

Require: $\left\langle T_i{}^j, L_i{}^j \right\rangle_{j=1}^{n}, PK^i{}_v$;

$Bill^i{}_v \leftarrow 0$;
for all $1 \leq j \leq n$ **do**;
$Bill^i{}_v \leftarrow Bill^i{}_v + g(T_i{}^j, L_i{}^j, NEW^{V_i}{}_{TV}{}^j)$;
End for;
Randomly choose $\lambda \in Z_q{}^*$;
$\Phi_1 \leftarrow \lambda \cdot P$;
$\Phi_2 \leftarrow \lambda \cdot PK^i{}_v$;
$\Re = Bill^i{}_v \cdot X_{\Phi_2} \bmod p$;
$\eta = \lambda - P_{pub} \cdot \Re \bmod q$;
$\sigma_{Bill^i{}_v} = \langle \Re || \eta || \Phi_1 \rangle$;
return $\sigma_{Bill^i{}_v}$;

Only those bills that pass the signature verification can be seen as a legitimate bill. For this purpose, the vehicle checks whether the equation $\Re \cdot P_{pub} + \eta \cdot P = SK^i{}_v \cdot \Phi_1{}'$ holds. The vehicle accepts the bill if the verification holds, and then recovers the toll bill $Bill^i{}_v$ by computing $Bill^i{}_v = \Re \cdot X^{-1}{}_{\Phi_2{}'} \bmod p$. Otherwise, the vehicle rejects it. The detailed signature verification process of the toll bill is provided in Algorithm 4.

Algorithm 4 Verification of the toll bill for each vehicle

Require: $\sigma_{Bill^i{}_v}, SK^i{}_v$;

$\Phi_1{}' \leftarrow \Re \cdot P_{pub} + \eta \cdot P$;
$\Phi_2{}' \leftarrow SK^i{}_v \cdot \Phi_1{}'$;
if $(\Phi_2{}' = \Phi_1{}')$ **then**
$Bill^i{}_v \leftarrow \Re \cdot X^{-1}{}_{\Phi_2{}'} \bmod p$;
return $Bill^i{}_v$;
else
return invalid signature;
end if;

6. Security Analysis

In this section, security analysis is presented to show that how our proposed scheme can satisfy our design objections and resist some attacks.

6.1. Correctness

- The signature messages generated by VSCs are correct and can resist threat model A mentioned in Section 4.2 if the system security parameters are correctly generated. The proof is as follows:

With system security parameters and signature messages generated by VSCs and vehicles, our proposed scheme can be proved to be correct as per the following equation.

$$\begin{aligned}\left(\sum_{i=1}^{n}\tau_i\cdot\sigma_i\right)\cdot P &= \left(\sum_{i=1}^{n}\tau_i\cdot(SK^i{}_{vsc}+\alpha_i\cdot\omega_i)\right)\cdot P\\ &=\sum_{i=1}^{n}(\tau_i\cdot AID_{vsc_i{}^1})+\sum_{i=1}^{n}(\tau_i\cdot\psi_i\cdot P_{pub})\\ &+\sum_{i=1}^{n}(\tau_i\cdot\alpha_i\cdot W_i)\\ &=\sum_{i=1}^{n}(\tau_i\cdot AID_{vsc_i{}^1})+\sum_{i=1}^{n}(\tau_i\cdot\psi_i)\cdot P_{pub}\\ &+\sum_{i=1}^{n}(\tau_i\cdot\alpha_i\cdot W_i)\end{aligned}\tag{5}$$

- The signature messages generated by vehicles are correct if the system security parameters are correctly generated.

With system security parameters and signature messages generated by vehicles, our proposed scheme can be proved to be correct as per the following equation.

$$\begin{aligned}&SK^i{}_{RSU}\cdot Sig_v{}^i\cdot P\\ &=SK^i{}_{RSU}\cdot(SK^i{}_v+z_i\cdot\Theta_1)\cdot P\\ &=SK^i{}_{RSU}\cdot SK^i{}_v\cdot P+SK^i{}_{RSU}\cdot z_i\cdot P\cdot\Theta_1\\ &=SK^i{}_{RSU}\cdot\Theta_2\cdot P+SK^i{}_{RSU}\cdot Z_i\ \cdot\Theta_1\\ &=DK+SK^i{}_{RSU}\cdot Z_i\cdot\Theta_1\end{aligned}\tag{6}$$

where $\Theta_1 = H_2(RID_{TCC}||RID_{RSU_i}||T_i||M)$, and $\Theta_2 = \hbar_i\cdot H_2(PID^i{}_v||\overline{\hbar_i}||T_i)+S$.

Theorem 1. *The signatures generated by VSCs and vehicles are unforgeable if all system parameters are created correctly.*

Proof of Theorem 1. Based on the threat model and design objections, the security model of our proposed scheme is defined by a game, which involves the interaction between a challenger ***C*** and an adversary ***A***. Assuming there exists an adversary ***A*** who can forge a valid signature, a challenger ***C***, who is able to solve the hardness of the *DL* problem with a non-negligible advantage, uses ***A*** as a subroutine. The detailed proof of our scheme is similar to the one in [38]. Due to space limitation, we omit it in this paper. □

6.2. Security Discussion

- Identity privacy preservation

The real identities of vehicles $RID^i{}_v$ are blinded by computing $\overline{\hbar_i} = \hbar_i\cdot P$ and $PID^i{}_v = RID^i{}_v\oplus H_1(S\cdot\overline{\hbar_i}||T_i)$. To obtain the real identities $RID^i{}_v$ from $PID^i{}_v$, the adversary must compute $S\cdot\overline{\hbar_i} = S\cdot\hbar_i\cdot P = \hbar_i\cdot P_{pub}$ from $P_{pub} = S\cdot P$. Therefore, due to the hardness of the CDH problem defined previously, we show that our proposed scheme can provide identity privacy preservation.

- Message authentication

In our scheme, the signature messages $\{\sigma_i, AID_{vsc_i}, T_i, L_i, W_i, LP_i\}$ where $\sigma_i = SK^i{}_{vsc}+\alpha_i\cdot\omega_i \bmod q$, $Sig_v{}^i = SK^i{}_v + z_i\cdot H_2(RID_{TCC}||RID_{RSU_i}||T_i||M) \bmod q$ generated by VSCs and vehicles during passing toll road can be checked by the TCC and RSUs, and the correctness of the equation verification is shown in Section 6.1. Using Section 6.1, the threat model B can be avoided in our proposed scheme.

- Conditional privacy preservation

The real identities of vehicles $RID^i{}_v$ are covered up by $PID^i{}_v = RID^i{}_v \oplus H_1(S \cdot \overline{\hbar_i}||T_i)$ where $\overline{\hbar_i} = \hbar_i \cdot P$. The TCC can perform an XOR operation as $RID^i{}_v = PID^i{}_v \oplus H_1(S \cdot \overline{\hbar_i}||T_i)$ using the system master private key S in an emergency or in the event of a disagreement to obtain vehicle real identities.

- Resisting impersonation attacks

Adversaries who want to impersonate a legitimate actor to reduce payment must generate a message $\{PID^i{}_v, C, T_i, Z_i, \overline{\hbar_i}\}$ satisfying the equation $SK^i{}_{RSU} \cdot Sig_v{}^i \cdot P = DK + Z_i \cdot SK^i{}_{RSU} \cdot H_2(RID_{TCC}||RID_{RSU_i}||T_i||M)$. As is shown in 6.1, RSUs can identify such an attack easily by checking whether Equation (6) holds. Therefore, any adversaries cannot impersonate a legitimate vehicle.

- Resisting modification attacks

$\{\sigma_i, AID_{vsc_i}, T_i, L_i, W_i, LP_i\}$ is a signature generated by VSCs fixed on pivotal toll roads. According to Theorem 1, the TCC can easily identify whether the signature $\{\sigma_i, AID_{vsc_i}, T_i, L_i, W_i, LP_i\}$ generated by VSCs has been modified by checking the equation $\sigma_i \cdot P = AID_{vsc_i}{}^1 + \psi_i \cdot P_{pub} + \alpha_i \cdot W_i$.

- Resisting man-in-the-middle attacks

Based on message authentication among entities such as VSCs, vehicles, and the TCC, we know that our proposed scheme can provide authentication for participants. Therefore, a man-in-the-middle attack can by resisted in our proposed scheme.

7. Performance Evaluation

In this section, the performance analysis of our proposed scheme is presented. To better demonstrate our proposed protocol intuitively, implementation with a pairing-based cryptography (PBC) library https://crypto.stanford.edu/pbc/ (accessed on 19 May 2021) and GNU Multiple Precision Arithmetic library on a Linux system using an Intel Core i5-9500 at a frequency of 3.0 GHz, and 8 GB of RAM are provided.

As illustrated in Figure 2, seven phases are separately named VSC enrollment, vehicle enrollment, RSU enrollment, message transmission of VSCs, message transmission of vehicles, message verification of RSUs, and TCC, respectively. It is not difficult to see that the time cost of vehicle enrollment is more than the other entities. Essentially, the vehicle needs to execute a point multiplication related to ECC, two additive operations, and three multiplication operations on Z_p in this phase. However, this takes a lot of time, so this phase can be executed offline ahead of time. Therefore, the amount of system time cost on execution is not burdensome.

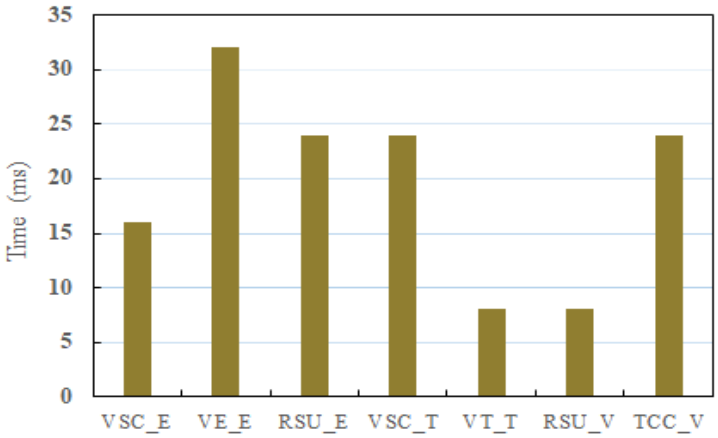

Figure 2. The overhead comparison among different phases of our scheme.

Figure 3 presents the time cost of signature verification. With the increase of the number of vehicles, the computation overheads of the RSU and TCC are increased. Essentially, each vehicle sends geolocation messages to the RSU and each VSC sends surveillance messages to the TCC, which leads to increased overheads. The reason that the time cost of the TCC is higher than the RSUs is that the TCC needs to execute three multiplication operations related to the ECC and an additive operation on Z_p.

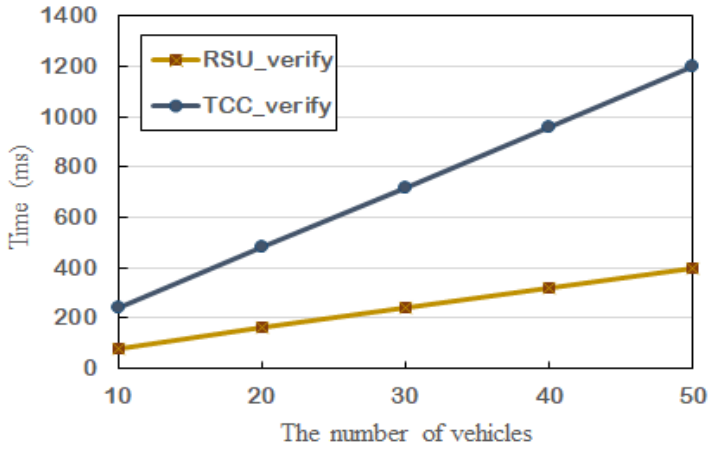

Figure 3. The time cost of signature verification.

To illustrate the superiority of our proposed scheme, the time costs of signature verification of different schemes are presented in Figure 4. Clearly, performance analysis shows that our scheme is much better than [38,39], i.e., the computation overheads in our scheme are much lower. Without using bilinear pairing, our proposed scheme can better meet the requirements of resource constraint in VANETs.

To cope with drivers who want to reduce payments or pay no bill by turning off his/her OBU, the performance of detection rates is evaluated. As shown in Figure 5, with the increase in vehicles, the detection rate increases slowly. Please note that the lowest detection rate of our scheme is still more than 89%, though the number of vehicles is 50.

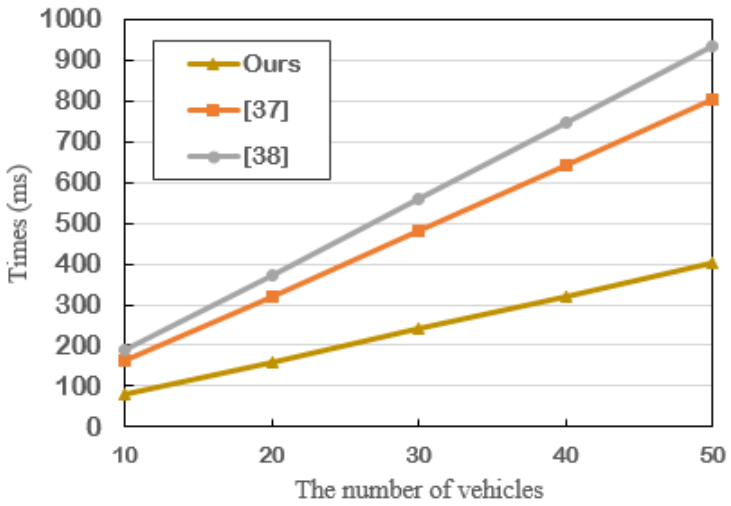

Figure 4. The time cost of signature verification of different schemes.

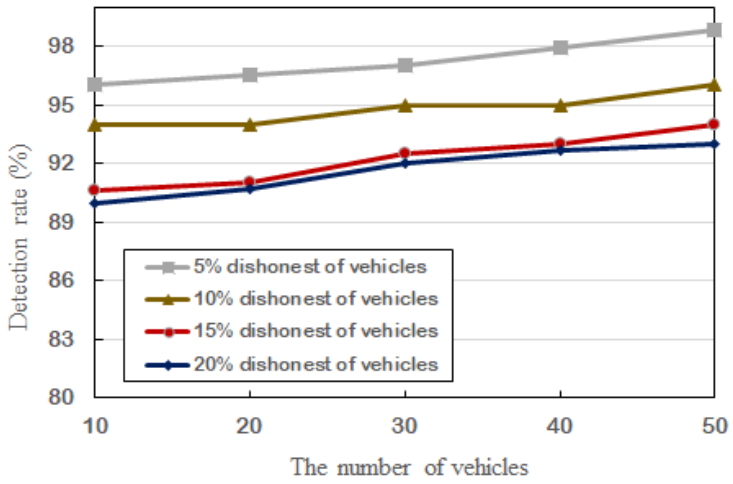

Figure 5. The detection rate and corresponding vehicles.

In fact, no more than 50 vehicles will pass through the toll road at the same time in the existing highway section. Therefore, our proposed scheme can be easily applied in practical application.

8. Conclusions

In this paper, a novel privacy-preserving road-pricing system with a trustworthiness evaluation scheme is proposed. In the scheme, we combine cryptographic primitives and our unique comparison method to force passing vehicles to behave honestly as much as possible. The PUF-based VSCs, which can resist various attacks such as man-in-the-middle, are used to record the real geolocation and corresponding time. Meanwhile, messages generated by the vehicle itself can be received by nearby RSUs and then be forwarded to the TCC, which compares whether they are equal. Moreover, a novel fuzzy comprehensive strategy trustworthiness evaluation approach is designed and applied to our proposed scheme to record vehicle misbehavior. Finally, sufficient theoretical and experimental analysis yields better performance in security and efficiency in comparison with previous schemes.

Author Contributions: Data curation, S.J. and Y.R.; Formal analysis, Y.R.; Investigation, Q.Z.; Methodology, J.S.; Resources, S.J.; Software, Q.Z.; Writing—original draft, Q.Z.; Writing—review & editing, Y.R. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China under Grants No. U1836115, No1922045, No1877034, the Natural Science Foundation of Jiangsu Province under Grant No. BK20181408, the Peng Cheng Laboratory Project of Guangdong Province PCL2018KP004, the CICAEET fund, and the PAPD fund.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wang, Y.; Ding, Y.; Wu, Q.; Wei, Y.; Qin, B.; Wang, H. Privacy-Preserving Cloud-Based Road Condition Monitoring With Source Authentication in VANETs. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 1779–1790. [CrossRef]
2. Qu, F.; Wu, Z.; Wang, F.; Cho, W. A Security and Privacy Review of VANETs. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 2985–2996. [CrossRef]
3. Bouchelaghem, S.; Omar, M. Reliable and secure distributed smart road pricing system for smart cities. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 1592–1603. [CrossRef]
4. Sheikh, M.S.; Liang, J.; Wang, W. A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs). *Sensors* **2019**, *19*, 3589. [CrossRef] [PubMed]
5. Saharan, S.; Bawa, S.; Kumar, N. Dynamic pricing techniques for Intelligent Transportation System in smart cities: A systematic review. *Comput. Commun.* **2020**, *150*, 603–625. [CrossRef]

6. Farouk, F.; Alkady, Y.; Rizk, R. Efficient Privacy-Preserving Scheme for Location Based Services in VANET System. *IEEE Access* **2020**, *8*, 60101–60116. [CrossRef]
7. Shen, J.; Wang, C.; Lai, J.; Xiang, Y.; Li, P. CATE: Cloud-Aided Trustworthiness Evaluation Scheme for Incompletely Predictable Vehicular Ad Hoc Networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 11213–11226. [CrossRef]
8. Shen, J.; Zhou, T.; Wei, F.; Sun, X.; Xiang, Y. Privacy-Preserving and Lightweight Key Agreement Protocol for V2G in the Social Internet of Things. *IEEE Internet Things J.* **2018**, *5*, 2526–2536. [CrossRef]
9. Zhang, J.; Yang, F.; Ma, Z.; Wang, Z.; Liu, X.; Ma, J. A Decentralized Location Privacy-Preserving Spatial Crowdsourcing for Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 2299–2313. [CrossRef]
10. Cui, J.; Wu, D.; Zhang, J.; Xu, Y.; Zhong, H. An Efficient Authentication Scheme Based on Semi-Trusted Authority in VANETs. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2972–2986. [CrossRef]
11. Chen, X.; Fonkwe, D.; Pang, J. Post-hoc user traceability analysis in electronic toll pricing systems. In *Data Privacy Management and Autonomous Spontaneous Security*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 29–42.
12. Popa, R.A.; Balakrishnan, H.; Blumberg, A.J. VPriv: Protecting Privacy in Location-Based Vehicular Services. In Proceedings of the 18th USENIX Security Symposium, Montreal, QC, Canada, 10–14 August 2009; Monrose, F., Ed.; USENIX Association: Berkeley, CA, USA, 2009; pp. 335–350.
13. Frederiksen, T.K.; Pinkas, B.; Yanai, A. Committed MPC—Maliciously Secure Multiparty Computation from Homomorphic Commitments. *IACR Cryptol. Eprint Arch.* **2017**, *2017*, 550.
14. Chaum, D.; Van Heyst, E. Group signatures. In *Workshop on the Theory and Application of of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1991; pp. 257–265.
15. Chen, X.; Lenzini, G.; Mauw, S.; Pang, J. A group signature based electronic toll pricing system. In Proceedings of the 2012 Seventh International Conference on Availability, Reliability and Security, Prague, Czech Republic, 20–24 August 2012; pp. 85–93.
16. Guo, J.; Baugh, J.P.; Wang, S. A group signature based secure and privacy-preserving vehicular communication framework. In Proceedings of the 2007 Mobile Networking for Vehicular Environments, Anchorage, AK, USA, 11 May 2007; pp. 103–108.
17. Jardí-Cedó, R.; Mut-Puigserver, M.; Castellà-Roca, J.; Magdalena, M.; Viejo, A. Privacy-preserving electronic road pricing system for multifare low emission zones. In Proceedings of the 9th International Conference on Security of Information and Networks, Newark, NJ, USA, 20–22 July 2016; pp. 158–165.
18. Shokri, R.; Troncoso, C.; Díaz, C.; Freudiger, J.; Hubaux, J. Unraveling an old cloak: k-anonymity for location privacy. In Proceedings of the 2010 ACM Workshop on Privacy in the Electronic Society, WPES 2010, Chicago, IL, USA, 4 October 2010; Al-Shaer, E., Frikken, K.B., Eds.; ACM: New York, NY, USA, 2010; pp. 115–118.
19. Buttyán, L.; Holczer, T.; Vajda, I. On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs. In Proceedings of the Security and Privacy in Ad-hoc and Sensor Networks, 4th European Workshop, Cambridge, UK, 2–3 July 2007; Lecture Notes in Computer Science; Stajano, F., Meadows, C.A., Capkun, S., Moore, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4572, pp. 129–141.
20. Gentry, C. Fully homomorphic encryption using ideal lattices. In Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, Bethesda, MD, USA, 31 May 2009; pp. 169–178.
21. Anderson, R.; Biham, E.; Knudsen, L. Serpent: A proposal for the advanced encryption standard. *NIST AES Propos.* **1998**, *174*, 1–23.
22. Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423. [CrossRef]
23. Schnorr, C. Efficient Signature Generation by Smart Cards. *J. Cryptol.* **1991**, *4*, 161–174. [CrossRef]
24. Boneh, D. Elgamal Digital Signature Scheme. In *Encyclopedia of Cryptography and Security*; van Tilborg, H.C.A., Ed.; Springer: Berlin/Heidelberg, Germany, 2005.
25. Alshammari, A.; Rawat, D.B. Intelligent Multi-Camera Video Surveillance System for Smart City Applications. In Proceedings of the IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019, Las Vegas, NV, USA, 7–9 January 2019; pp. 317–323.
26. Chatterjee, U.; Govindan, V.; Sadhukhan, R.; Mukhopadhyay, D.; Chakraborty, R.S.; Mahata, D.; Prabhu, M.M. Building PUF Based Authentication and Key Exchange Protocol for IoT Without Explicit CRPs in Verifier Database. *IEEE Trans. Dependable Secur. Comput.* **2019**, *16*, 424–437. [CrossRef]
27. Zhou, J.; Cao, Z.; Qin, Z.; Dong, X.; Ren, K. LPPA: Lightweight Privacy-Preserving Authentication From Efficient Multi-Key Secure Outsourced Computation for Location-Based Services in VANETs. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 420–434. [CrossRef]
28. Zhou, J.; Dong, X.; Cao, Z.; Vasilakos, A.V. Secure and privacy preserving protocol for cloud-based vehicular DTNs. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1299–1314. [CrossRef]
29. Shen, J.; Liu, D.; Chen, X.; Li, J.; Kumar, N.; Vijayakumar, P. Secure Real-Time Traffic Data Aggregation With Batch Verification for Vehicular Cloud in VANETs. *IEEE Trans. Veh. Technol.* **2020**, *69*, 807–817. [CrossRef]
30. Saxena, N.; Shen, H.; Komninos, N.; Choo, K.R.; Chaudhari, N.S. BVPSMS: A Batch Verification Protocol for End-to-End Secure SMS for Mobile Users. *IEEE Trans. Dependable Secur. Comput.* **2020**, *17*, 550–565. [CrossRef]
31. Limbasiya, T.; Das, D. ESCBV: Energy-efficient and secure communication using batch verification scheme for vehicle users. *Wirel. Netw.* **2019**, *25*, 4403–4414. [CrossRef]

32. Li, K.; Lau, W.F.; Au, M.H. A Secure and Efficient Privacy-Preserving Authentication Scheme for Vehicular Networks with Batch Verification Using Cuckoo Filter. In Proceedings of the Network and System Security—13th International Conference, NSS, Sapporo, Japan, 15–18 December 2019; Lecture Notes in Computer Science; Liu, J.K., Huang, X., Eds.; Springer: Berlin/Heidelberg, Germany, 2019; Volume 11928, pp. 615–631.
33. Bayat, M.; Barmshoory, M.; Rahimi, M.; Aref, M.R. A secure authentication scheme for VANETs with batch verification. *Wirel. Netw.* **2015**, *21*, 1733–1743. [CrossRef]
34. Horng, S.; Tzeng, S.; Pan, Y.; Fan, P.; Wang, X.; Li, T.; Khan, M.K. b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1860–1875. [CrossRef]
35. Zhang, J.; Xu, M.; Liu, L. On the Security of a Secure Batch Verification with Group Testing for VANET. *Int. J. Netw. Secur.* **2014**, *16*, 355–362.
36. Su, Y.S.; Wu, S.Y. Applying data mining techniques to explore user behaviors and watching video patterns in converged IT environments. *J. Ambient. Intell. Humaniz. Comput.* **2021**. [CrossRef]
37. Su, Y.S.; Suen, H.Y.; Hung, K.E. Predicting behavioral competencies automatically from facial expressions in real-time video-recorded interviews. *J. Real-Time Image Process* **2021**. [CrossRef]
38. He, D.; Zeadally, S.; Xu, B.; Huang, X. An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691. [CrossRef]
39. Shim, K. CPAS: An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks. *IEEE Trans. Veh. Technol.* **2012**, *61*, 1874–1883. [CrossRef]