symmetry

MDPI

Article

TPM-Based Conditional Privacy-Preserving Authentication Protocol in VANETs

Mingwu Zhang [1,2,*], Boyao Zhu [1], Yumei Li [1] and Yuntao Wang [3]

[1] School of Computers, Hubei University of Technology, Wuhan 430068, China; byzhu@hbut.edu.cn (B.Z.); yumei_li@hbut.edu.cn (Y.L.)
[2] Xiangyang Industrilal Institute of Hubei University of Technology, Xiangyang 441000, China
[3] Graduate School of Engineering, Osaka University, Osaka 565-0871, Japan ; wang@comm.eng.osaka-u.ac.jp
* Correspondence: mzhang@hbut.edu.cn

Abstract: With the establishment of intelligent transportation systems (ITS), research on vehicle ad-hoc networks (VANETs) has played an irreplaceable role in improving traffic safety and efficiency. However, because the deployment of devices based on the IoV is in an open field, the IoV is extremely vulnerable to various attacks without security protection, e.g., remote intrusion, control, trajectory tracking, etc. In order to avoid the above-mentioned attacks and resource abuses, provably secure cryptography primitives are generally considered to guarantee and realize the security of VANETs. This paper proposes a TPM-based conditional privacy-preserving authentication protocol (T-CPPA) which achieves both the integrity and the authenticity of the message/instruct content. The vehicle's privacy is protected by embedding the system master private key into the trust platform module (TPM) which is responsible for generating pseudonyms and signature keys. The authenticity of message content is ensured by calculating message similarity in a cluster-based model. We give the concrete construction of our T-CPPA authentication scheme in symmetric bilinear groups and design a batch validation algorithm to improve efficiency. Security analysis shows that our scheme can resist various traditional attacks in VANETs, and the experimental results indicate that our scheme is efficient and useful in practice.

Keywords: conditional privacy-preserving; batch authentication; cluster; trusted platform module

Citation: Zhang, M.; Zhu, B.; Li, Y.; Wang, Y. TPM-Based Conditional Privacy-Preserving Authentication Protocol in VANETs. *Symmetry* **2022**, *14*, 1123. https://doi.org/10.3390/sym14061123

Academic Editor: José Carlos R. Alcantud

Received: 6 April 2022
Accepted: 24 May 2022
Published: 30 May 2022

1. Introduction

With the rapid development of the internet and communication technology, vehicle ad hoc networks (VANETs or IoV, we will use IoV and VANETs commutatively in this work) have become one of the most popular applications in the field of the Internet of Things [1,2]. Through wireless communication devices, vehicles can effectively apply all the dynamic information in the network to improve road safety. For example, by receiving information from near vehicles, a vehicle can learn about road conditions in advance and then provide sufficient response time for the driver or intelligent assistance system [3].

The typical structure of VANETs consists of a trust authority (TA), a roadside unit (RSU) and a vehicle equipped with various sensors and an on-board unit (OBU). The vehicles utilize wireless communication technology [4] to report road condition information at specific time intervals, such as congestion, location, speed, direction, weather, and accident status. RSU is responsible for receiving road condition information and verifying the information. Meanwhile, RSU forwards the road condition to the traffic control center so that the control center can make reasonable strategies to improve the traffic efficiency.

Because messages are transmitted on open channels in IoV, the system will face various potential attacks, posing a huge challenge to the security of the IoV [5]. For example, in order to keep its road clear, a malicious vehicle may broadcast false messages (or modify messages sent by other vehicles) to whole entities in VANETs, causing other vehicles to detour. Therefore, it is necessary to guarantee the integrity of the message and verify the identity of the sender. Moreover, the privacy of the vehicle is also a concern, e.g., the vehicle's identity and driving track.

We believe that it is not enough to only verify the integrity of the message and the legal identity of the sender in VANETs, because even a legitimate user may also do things that harm the system for the sake of profit. In the transportation network, a piece of false information is likely to bring fatal disasters, so we want to increase the fault tolerance of the system via real-time detection of false information.

Among the existing authentication schemes, schemes [6–10] verify the legal identity of the message sender and ensure the integrity of the message by using cryptographic knowledge, which lacks the authenticity of the message content and identification of variant vehicles. In addition, when it comes to revoking users, these schemes also have problems with revoking users. Schemes [11–15] design a reputation system for VANETs, which aims to guarantee the authenticity of the message content to a certain extent, but the vehicle needs to frequently query the credibility of the message sender from trusted institutions, resulting in huge communication overhead.

For the shortcomings of existing solutions, an identity-based signature scheme is designed to verify the integrity of the message. And we divide the large IoV into several clusters inspired by [16]. Each cluster selects a vehicle as the cluster head, and the cluster head summarizes the road condition information to ensure the authenticity of the message content. The main contributions of our scheme are listed as follows:

(1) We propose a conditional privacy-preserving authentication scheme for VANETs, exploiting clusters to divide the large VANETs into smaller networks to unify messages, which greatly improves the stability of the system.
(2) We provide a batch authentication algorithm, in which we can aggregate the signatures of multiple messages and verify through one bilinear pairing to improve the verification efficiency.
(3) We provide a comprehensive security analysis to prove that our scheme ensures security, and demonstrate that our scheme is feasible in terms of computational overhead and security requirements compared with other existing schemes through extensive experiments and comparisons.

The rest of the paper is organized as follows: In Section 2 we summarize and review the related work. In Section 3 we introduce the problem statement, preliminary knowledge, and system mode. In Section 4 we provide a cluster head selection algorithm and safety certification protocol for vehicles. We present the security analysis in Section 5. In Section 6, we give the experimental results of the scheme, and we summarize our work in Section 7.

2. Related Work

So far, many authentication schemes have been proposed to secure VANETs. In [17–19], the anonymous certificates were used to realize privacy preservation authentication, where the OBU needed to preload many key pairs and corresponding certificates. During communication, the vehicle fulfilled authentication and integrity by choosing a public/secret-key pair every time. However, both TA and vehicle stored a large number of digital certificates that cost a vast physical resource. Furthermore, the system needed to maintain a certificate revocation list (CRL), and the time consumption of signature verification would be seriously affected when the CRL became large. Zhong et al. [20] developed a certificateless privacy-preserving aggregated signatures scheme in VANETs for secure vehicle-to-infrastructure (V2I) communication. However, more bilinear pairing operations were used during verification, which reduced the verification efficiency. Xiong et al. [21] implemented a dual-insurance authentication scheme, in which a malicious adversary could not conduct a forgery attack when the vehicle leaked part of the private key, but it required improvement in protecting vehicle privacy. Wei et al. [22] presented a privacy-preserving multi-modal implicit authentication protocol. The privacy of the vehicle was protected, and the identity of the vehicle was verified by combining the behavior feature vector of the vehicle with the matrix operations.

In order to ensure the authenticity of the message, some existing schemes constructed trust evaluation models based on the IoV. Liu et al. [23] proposed a dual authentication trust model, which evaluated each other's vehicle reputation by the historical interaction behavior between vehicles. Each vehicle had to deliver the score to TA to update the reputation score of the vehicle. Huang et al. [24] provided a scheme to evaluate the reliability of data by comparing the opinions of neighboring vehicles with a high weight of proximity to the event. Zhou et al. [25] introduced a security authentication scheme based on data trust assessment, according to direct and indirect trust assessment for security authentication. However, the drawbacks of these reputation assessment schemes are obvious, with frequent interactions causing high latency and high communication overhead in the system.

Vehicles can use multiple pseudonyms to protect their privacy. He et al. [26] made the vehicle's OBU store a set of pseudonyms during the registration phase, but this method requires that the pseudonyms must have an expiration date and requires the vehicle to have a certain storage capacity. In order to relieve the pressure of pseudonyms on the storage performance of vehicles, Wang et al. [27] applied pseudonym exchange technology to protect the privacy of vehicles, where vehicles exchanged pseudonyms through encrypted channels so that pseudonyms could be reused. Liu et al. [28] let vehicles use homomorphic encryption technology to generate an arbitrary number of pseudonyms in a blockchain-based system to achieve unlinkability. Tzeng et al. [29] embedded the system master key into the TPM for generating the pseudonym and signing key, which reached conditional privacy protection. Other schemes [30–32] used group signature technology to protect the privacy of vehicles. The group signature scheme can achieve anonymity in secure authenticated messages, satisfying conditional privacy protection to provide secure communication. Each group member can sign messages on behalf of the entire group without revealing their real identity. However, the latency of these schemes is linearly proportional to the number of revocation vehicles. Therefore, they may not perform well in large-scale networks such as VANETs.

A comparison of some representative schemes is shown in Table 1. In the existing IoV systems, researchers either only focus on the message integrity in the communication and the sender's identity, or only on the credibility of the message. Furthermore, vehicles interact frequently with other entities in existing schemes for assessing the credibility of message content, which significantly increases the delay and communication overhead of the system. To guarantee both message integrity and authenticity of the message content in the complex IoV scenarios and reduce vehicle communication overhead, we propose the T-CPPA scheme.

We use an elliptic cryptographic curve system with the help of TPM hardware security to implement the identity-based signature algorithm and protect the privacy of vehicles. By calculating the distance [22,33,34] of the message vector in the cluster, the scheme can ensure the authenticity of message content and improve the fault tolerance rate of the system.

Table 1. Overview of existing schemes on VANETs.

Category	Scheme	Method	Limitation
Message authentication	Asghar et al. [19]	Utilize anonymous certificates to reach message authentication	Vast digital certificates cause huge storage burden
	zhong et al. [20]	Propose a certificateless authentication scheme to ease storage burden	Multiple bilinear pairing operations reduce the verification efficiency
	Wei et al. [22]	Apply matrix operations to accomplish message authentication	The characteristics of the matrix will bring high communication overhead

Table 1. *Cont.*

Category	Scheme	Method	Limitation
Message credibility	Liu et al. [23]	Evaluate reputation in cars that have interacted with each other	Frequent interactions cause high latency and communication overhead
	Huang et al. [4]	Evaluate the reliability of data by comparing the opinions of neighboring vehicles with a high weight of proximity to the event	
	Zhou et al. [25]	According to direct and indirect trust assessment for security authentication	
Privacy preservation	He et al. [26]	Store a set of pseudonyms in OBU during the registration phase	The pseudonym has an expiration date and requires the OBU to have a certain storage capacity
	Guo et al. [31]	Use group signature technology to achieve anonymity in secure authenticated messages	The scheme latency is linearly proportional to the number of revocation vehicles

3. Preliminary and Framework Description

3.1. Symmetric Bilinear Pairings

Symmetric Bilinear Pairings: Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be the additive group and multiplicative group of order q, respectively. A bilinear e is a map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, and satisfies the following three conditions:

1. *Bilinearity*. For all $P, Q \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_q^*$, $e(aP, bQ) = e(P, Q)^{ab}$;
2. *Non-degeneracy*. For each $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_1$, $e(g_1, g_2) \neq 1$;
3. *Computability*. There exits an efficiently computable algorithm for computing map e.

Computational Diffie–Hellman (CDH) problem: Given $P, aP, bP \in \mathbb{G}_1$ as described above for unknown $a, b \in \mathbb{Z}_q^*$, the goal of the problem is to find abP. The CDH problem is $(t - \varepsilon)$ hard, if there exists no probabilistic polynomial time algorithm $\mathcal{A}$ that can solve the CDH problem in time at most t with probability ε as

$$Adv_{\varepsilon} = \Pr[abP \leftarrow \varepsilon(P, aP, bP) : a, b \in \mathbb{Z}_q^*] \geq \varepsilon.$$

3.2. TPM and Trusted Computing Technology

Trusted computing is promoted and developed by the Trusted Computing Group (TCG), which is committed to solving the trusted computing problem in the field of information security by integrating TPM as the root of trust for any device. The TPM specification has been upgraded to 2.0. Figure 1 shows the main components and module structure.

In this paper, we injected the system master private key into the TPM and embed a piece of program code. The TPM of each vehicle generates pseudonyms and signature keys for the vehicle. We believe that TPM is completely credible.

3.3. System Model

The system model of the proposed T-CPPA protocol for cluster-based IoV is presented in Figure 2, which is comprised of the following roles.

- **TA**: The TA is a trusted third party with high storage and communication capabilities. It is responsible for generating system parameters and preloading them in the OBU of the vehicle offline. In addition, it can dynamically revoke the legal identity of the vehicle based on the behavior of the vehicle, so that the vehicle cannot interact with other members.
- **RSU**: RSU is a wireless communication device deployed at the roadside using DSRC protocol, mainly responsible for broadcasting and relaying, and ensuring stable vehicle communication within range.
- **Cluster head**: The cluster head is the agent vehicle of the cluster. It is responsible for collecting the road condition information from other vehicles in the cluster and

communicating with the RSU. What's more, it monitors the vehicles in the cluster. It is the communication hub between the vehicles in the cluster and the RSU.

- **Vehicle**: The vehicles are equipped with a positioning system that allows the cluster head to track the position of the vehicles at any time. In addition, when the cluster is canceled for various reasons, the vehicles in the cluster will reselect the cluster head.

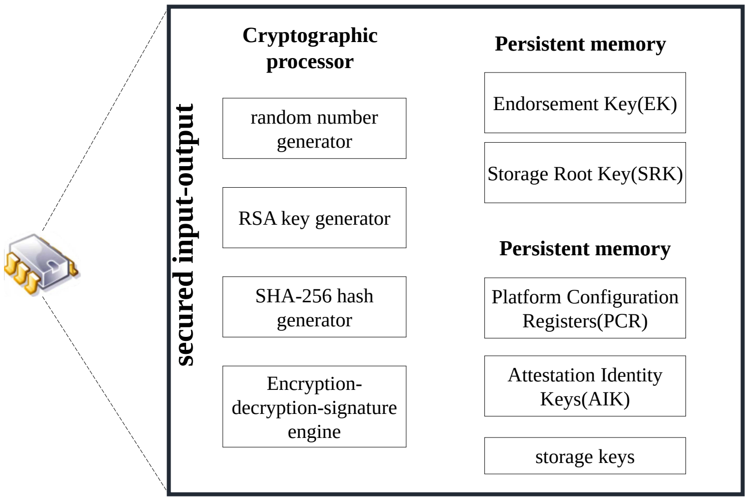

Figure 1. Main structure of TPM [35].

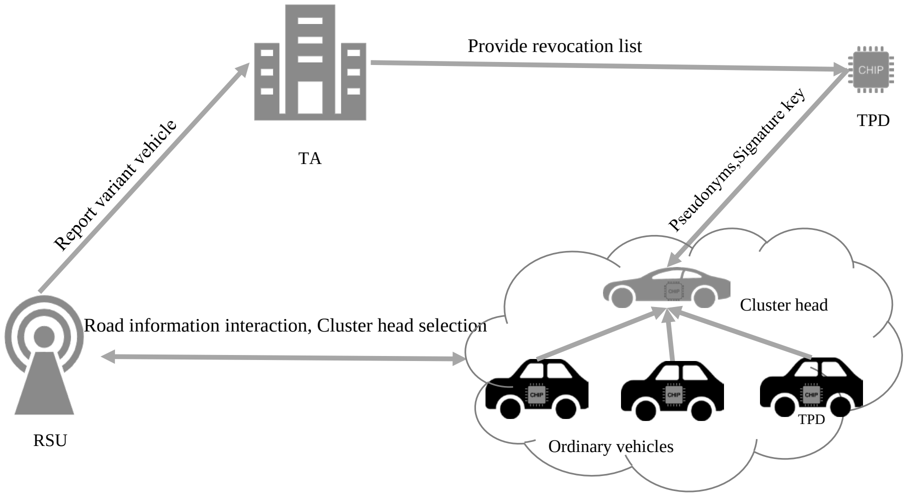

Figure 2. System framework.

TA is the control center of the entire system, granting legal identities to all vehicles in the system. RSU provides traffic information for vehicles entering its range, assigns vehicles to a particular cluster, or makes vehicles become cluster heads. The cluster head collects and processes the traffic information fed back by the vehicles in the cluster and sends it to the RSU. At the same time, it also monitors the vehicles in the cluster. Each cluster is independent of the other.

In this paper, TA is a fully trusted entity and will not be destroyed. RSU is semi-honest. In addition, we assume that most of the vehicles in the system are also honest.

3.4. Security and Privacy Requirement

- **Message Authentication**: The receiver (such as RSU or other vehicles) should have the ability to verify messages sent from other vehicles to ensure the integrity of the message.

- **Batch Authentication**: It is inefficient to verify the received messages one by one, so batch verification needs to be introduced to verify multiple messages at once, which improves the efficiency of the system and saves computational cost.
- **Resilient to Replay Attack**: The attacker will steal the communication message and resend the message at a later time, and a secure IoV system should be able to withstand this kind of attack.
- **Resilient to Masquerade Attack**: The attacker may pretend to be legitimate user and send false information to members of the system in order to achieve their own goals.
- **Resilient to Message Modification Attack**: The attacker intercepts the sender's information and selectively modifies the content of the data to impersonate the sender.
- **Resilient to Linkability Attack**: The attacker cannot distinguish whether two messages are from the same sender.

4. The Detailed Construction

4.1. Overview

Our scheme mainly consists of three parts. The first part is cluster formation and selection, the second part is security authentication, and the third part is message similarity detection, which is explained in detail in Section 6.

In the first part, RSU judges whether external vehicles can join the cluster by calculating the fit values of vehicles in a certain cluster. After a new vehicle joins the cluster, the RSU executes the cluster head selection algorithm and determines whether to update the cluster head by calculating the cluster head factor.

The working flow of the second part is illustrated in Figure 3. In the system initialization stage, the TA generates system parameters. In the registration stage, the TA embeds the system master key into the TPM of the vehicle. The vehicle requests a pseudonym and a signature key from the TPM when sending a message every time, and the TA also generates a public–private key pair for the RSU. In the request for cluster head/join the cluster stage, the vehicle sends its status information and signature to the RSU. In the information-exchange stage, the vehicle in the cluster sends the road condition information and signature to the cluster head. In the verification stage, the cluster head summarizes the information within the cluster and detects whether there are variant vehicles, and returns the information to RSU.

We give the key symbols that appear in the scheme in Table 2.

Table 2. Notations.

Parameter	Value
TA	trust authority
RSU	road-side unit
TPM	Trust platform module
c_i	cluster head factor
V_{prop}	indicates the type of vehicle, such as private cars, government cars, public buses, official cars
v_i	speed of the *i*-th vehicle
$\bar{v}$	average speed of the vehicles in the cluster
s_i	distance of vehicle will travel on the current road
d_i	distance between the vehicle and fog head
R	vehicle's broadcast range
h_i	cluster head factor
n_i	number of neighboring vehicles
$\mathbb{G}_1, \mathbb{G}_2, e(\cdot), P_{pub}$	system parameters
$H_1(\cdot), H_2(\cdot), H_3(\cdot), H_4(\cdot)$	hash function
ID_v, ID_R	ID of vehicle and RSU
$AID_{i,1}, AID_{i,2}$	the first pseudonym and the second pseudonym of the *i*-th vehicle
sk_{v_i}	private key of the *i*-th vehicle
sk_R, pk_R	RSU's private key and public key
$TS1, TS2$	timestamp
$\|\|$	message concatenation operation

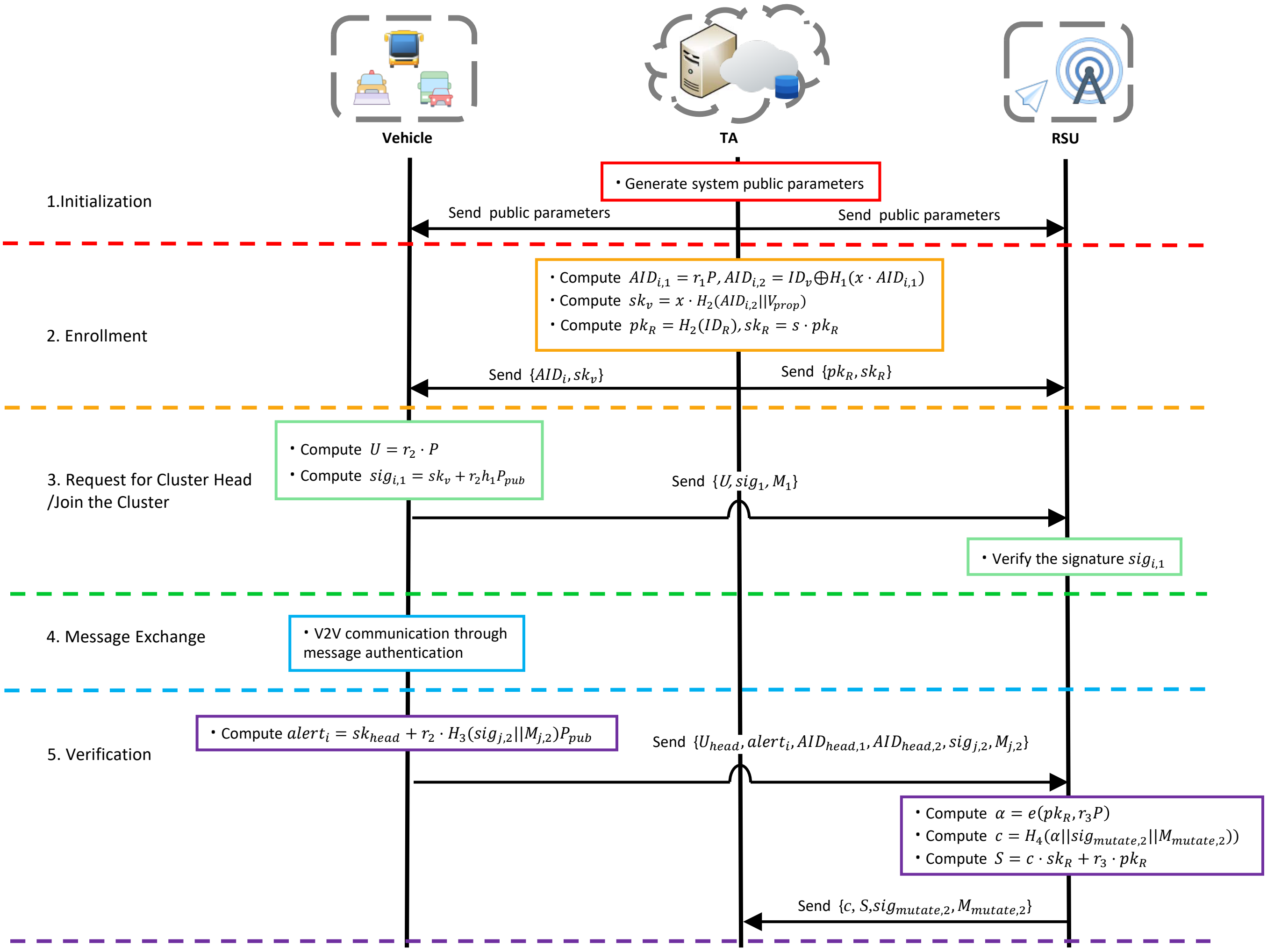
Vehicle
TA
RSU
1.Initialization
• Generate system public parameters
Send public parameters
Send public parameters
2. Enrollment
• Compute $AID_{i,1} = r_1P, AID_{i,2} = ID_v \oplus H_1(x \cdot AID_{i,1})$
• Compute $sk_v = x \cdot H_2(AID_{i,2}||V_{prop})$
• Compute $pk_R = H_2(ID_R), sk_R = s \cdot pk_R$
Send $\{AID_i, sk_v\}$
Send $\{pk_R, sk_R\}$
3. Request for Cluster Head /Join the Cluster
• Compute $U = r_2 \cdot P$
• Compute $sig_{i,1} = sk_v + r_2h_1P_{pub}$
Send $\{U, sig_1, M_1\}$
• Verify the signature $sig_{i,1}$
4. Message Exchange
• V2V communication through message authentication
5. Verification
• Compute $alert_i = sk_{head} + r_2 \cdot H_3(sig_{j,2}||M_{j,2})P_{pub}$
Send $\{U_{head}, alert_i, AID_{head,1}, AID_{head,2}, sig_{j,2}, M_{j,2}\}$
• Compute $\alpha = e(pk_R, r_3P)$
• Compute $c = H_4(\alpha||sig_{mutate,2}||M_{mutate,2}))$
• Compute $S = c \cdot sk_R + r_3 \cdot pk_R$
Send $\{c, S, sig_{mutate,2}, M_{mutate,2}\}$

Figure 3. Detail protocol of our T-CPPA scheme.

4.2. Cluster Head Selection Algorithm

Cluster Head Selection: From the perspective of public trust, we assume that people's trust in buses, government cars, official cars, and private cars goes from high to low. Then we define the degree of fit between a certain vehicle and a cluster:

$$c_i = a * (\frac{v_i - \bar{v}}{\bar{v}})^2 + b * \frac{1}{s_i} + c * \frac{d_i}{R} \tag{1}$$

where a, b and c are weighting factors, and we set $a + b + c = 1$. From Equation (1), we can see that the smaller the difference between the vehicle speed v_i and the average vehicle speed in the cluster, the longer the distance traveled on the current road, and the closer the distance between the vehicle and the cluster head, the smaller the fit between the vehicle and the cluster. Therefore, the higher the behavioral consistency between the vehicle and the vehicles in the cluster, the greater the probability of joining the cluster.

After the vehicle enters the specified range, RSU first helps it select the appropriate cluster. If the fit degree reaches the preset threshold, the vehicle will join the cluster; otherwise, RSU calculates the cluster head factor for the vehicle to determine whether the vehicle can become the cluster head. We first arrange the priority of the vehicle cluster heads in order of buses, government cars, official cars, and private cars. Then we define the cluster heads factor:

$$h_i = e * (\frac{1}{s_i})^2 + f * \frac{1}{n_i + 1}. \tag{2}$$

For the same reason as a, b, and c mentioned above, we also set $e + f = 1$. From Formula (2), we can see that the more vehicles that are covered by the one-hop communication range of the cluster head, the more stable the driving state of the entire cluster will be.

As shown in Figure 4, to control sequence, cars A and B are right-bound buses and a down police car, respectively, and the rest are ordinary vehicles. The yellow circle and the blue circle represent the communication range of vehicles a and b, respectively, and the black circle represents the coverage of the RSU. Take a cluster with vehicle A as the cluster head as an example. If a car wants to join the cluster, it needs to calculate its fit with this cluster. The fitness function is to distinguish whether the vehicle can join the cluster. When the driving direction of the vehicle and the cluster are in opposition, or the speed is very different from the average speed of the cluster, the vehicle is far away from the cluster head, then the cluster head refuses the vehicle to join the cluster.

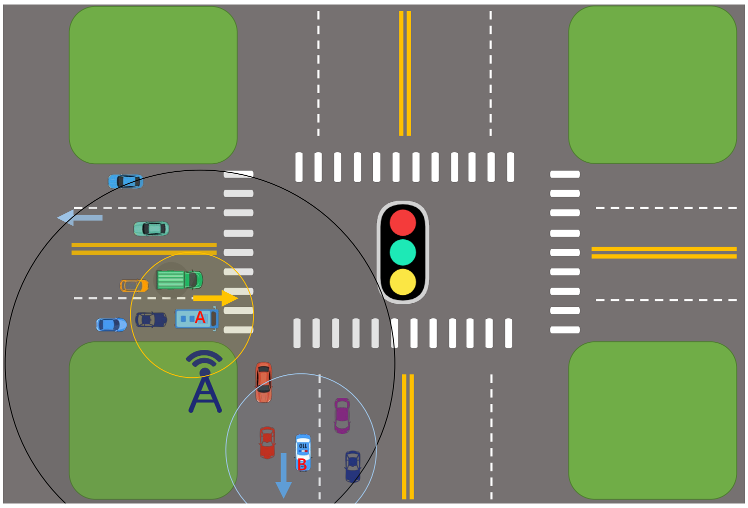

Figure 4. Illustation of cluster head selection.

In this paper, when we select the cluster head, we first filter according to the attributes of the vehicle, and then calculate whether the cluster head factor can reach the threshold. In order to balance performance and energy consumption, we set the threshold to 0.5. The vehicle-cluster fit algorithm runs on the vehicle and the cluster head selection algorithm runs on the RSU.

4.3. Security Authentication and Message Management

We now define the security authentication and message processing algorithms. The purpose of this algorithm is to allow only vehicles with legal identities to interact with RSUs or other vehicles. In addition, the cluster head can detect the variant vehicles in real time. Then our algorithms are as follows.

System Initialization Stage: This stage is done by the TA as below.

1. TA selects a security parameter κ.
2. TA selects two elliptic cryptographic curve groups $\mathbb{G}_1$ and $\mathbb{G}_2$, where $\mathbb{G}_1$ is an additive group and $\mathbb{G}_2$ is a multiplicative group. What's more, the order of the elliptic cryptographic curve $q > 2^{\kappa}$.
3. TA randomly chooses a master private key $x \in \mathbb{Z}_q^*$ and P which is the generator of $\mathbb{G}_1$,compute the system public key $P_{pub} = x \cdot P$.

4. TA picks four hash functions $H_1 : \mathbb{G}_1 \to \{0,1\}^n$, and $H_2 : \{0,1\}^* \to \mathbb{G}_1$, and $H_3 : \{0,1\}^* \to \mathbb{Z}_q^*$, and $H_4 : \mathbb{G}_2 \to \{0,1\}^n$.

Then the public parameters $param$ is defined as $\{\mathbb{G}_1, \mathbb{G}_2, q, P, P_{pub}, H_1, H_2, H_3, H_4\}$.

Enrollment Stage: This phase includes the registration of the RSU and the registration of the vehicle. The user should drive his/her vehicle to TA for registration.

1. TA obtains the identity number ID_v and makes a judgment on the attributes V_{prop} of the vehicle, Then TA loads the parameters $\{\mathbb{G}_1, \mathbb{G}_2, q, P, P_{pub}, H_1, H_2, H_3, H_4, x\}$ on the TPM of each vehicle. Every time the vehicle sends a message to the other parties, it will first request service from the built-in TPM.
2. The RSU provides its identity number ID_R to the TA, TA computes $pk_R = H_1(ID_R)$ and store it in the local, then TA computes $sk_R = x \cdot pk_R$ and send it to RSU through a secure channel.

Request for Cluster Head Stage: When a vehicle enters the range of an RSU, it searches for clusters within the current range. If there is a cluster that meets the conditions to join the cluster, it sends a message to the cluster head asking to be a member of the cluster. If not, the vehicle applies to the RSU to become a cluster head.

1. TPM selects a random number $r_{i,1}$,then it computes pseudonym $AID_i = (AID_{i,1}, AID_{i,2}, TS_1)$ where $AID_{i,1} = r_{i,1} \cdot P$, $AID_{i,2} = ID_v \oplus H_1(x \cdot AID_{i,1})$ and signature key $sk_{v_i} = x \cdot H_2(AID_{i,2} \parallel V_{prop} \parallel TS_1)$.
2. The vehicle obtains the pseudonyms and signature key from the built-in TPM.
3. Vehicle i selects a random number $r_{i,2}$ and computes $U_i = r_{i,2} \cdot P$, the signature $sig_{i,1} = sk_{v_i} + r_{i,2} \cdot h_{i,1} \cdot P_{pub}$, where $M_{i,1} = (m_{i,1}, V_{prop}, AID_i, TS_2)$, $h_{i,1} = H_3(M_{i,1})$, $m_{i,1}$ includes the speed, direction and position of the vehicle.
4. The vehicle sends (U_i,$sig_{i,1}$,$M_{i,1}$) to the RSU.
5. The RSU checks whether $TS_2 - TS_1$ is within a reasonable range. If not, RSU rejects the message and aborts the algorithm.
6. The RSU verifies the signature: $e(P, sig_{i,1}) \overset{?}{=} e(P_{pub}, H_2(AID_{i,2} \parallel V_{prop} \parallel TS_1) + h_{i,1} \cdot U_i)$
7. If the authentication succeeds, the RSU executes the cluster head selection algorithm; otherwise, the request is rejected.

The correctness of the authentication equation is demonstrated as follows:

$$\begin{aligned} e(P, sig_{i,1}) &= e(P, sk_{v_i} + r_{i,2} \cdot h_{i,1} \cdot P_{pub}) \\ &= e(P, x \cdot H_2(AID_{i,2} \parallel V_{prop} \parallel TS_1) + x \cdot r_{i,2} \cdot h_{i,1} \cdot P) \\ &= e(P_{pub}, H_2(AID_{i,2} \parallel V_{prop} \parallel TS_1) + r_{i,2} \cdot h_{i,1} \cdot P) \\ &= e(P_{pub}, H_2(AID_{i,2} \parallel V_{prop} \parallel TS_1) + h_{i,1} \cdot U_i) \end{aligned} . \tag{3}$$

Join the Cluster Stage: The vehicle finds a suitable cluster and requests the cluster head to join them.

1. In this stage, the message sent by the vehicle to the cluster head is similar to ***Request for Cluster Head Stage***, so details are not provided
2. The cluster head verifies the signature. If validated, the vehicle joins the small LAN set up by the cluster to prepare for the next phase of communication; Otherwise, the cluster head rejects the vehicle's request.

Message Exchange Stage: In the cluster, the vehicle sends traffic information to the cluster head. The cluster head processes the received information and finally sends the traffic information to the RSU. If any vehicle is detected to be mutated, it reports the mutated vehicle to the RSU.

1. Vehicles request the pseudonyms and signature key from their TPMs respectively.
2. The vehicles in the cluster sign the traffic information $sig_{i,2} = sk_{v_i} + r_{i,2} \cdot h_{i,2} \cdot P_{pub}$, where $h_{i,2} = H_3(M_{i,2})$ and $M_{i,2} = (m_{i,2}, AID_i, TS2)$, $m_{i,2}$ includes the vehicle's speed, direction, location, and nearby road conditions.
3. The vehicle i sends ($sig_{i,2}$,$M_{i,2}$) to its cluster head.

4. The cluster head checks whether $TS_2 - TS_1$ is within a reasonable range. If not, the the cluster head rejectes and aborts the algorithm.
5. Considering that the cluster head receives more information at one time, batch verification is adopted to improve efficiency: $e(P, \sum_{i=1}^{n} sig_{i,2}) \overset{?}{=} e(P_{pub}, \sum_{i=1}^{n}[H_2(AID_{i,2} \parallel V_{prop}) + h_{i,2} \cdot U_i])$.

The correctness of the batch authentication is

$$\begin{aligned} e(P, \sum_{i=1}^{n} sig_{i,2}) &= e(P, \sum_{i=1}^{n}[sk_{v,i} + r_{i,2} \cdot h_{i,2} \cdot P_{pub}]) \\ &= e(P, \sum_{i=1}^{n}[H_2(AID_{i,2} \parallel V_{prop} \parallel TS_1) + r_{i,2} \cdot h_{i,2} \cdot P])^x \\ &= e(P_{pub}, \sum_{i=1}^{n}[H_2(AID_{i,2} \parallel V_{prop} \parallel TS_1) + r_{i,2} \cdot h_{i,2} \cdot P]) \\ &= e(P_{pub}, \sum_{i=1}^{n}[H_2(AID_{i,2} \parallel V_{prop} \parallel TS_1) + h_{i,2} \cdot U_i]) \end{aligned} . \quad (4)$$

Report Variant Vehicle Stage: After RSU receives the report of the cluster head on the mutant vehicle, RSU performs batch verification through formula (4). After the verification is passed, RSU signs the mutant vehicle and sends it to TA. TA then puts the pseudonym of the variant vehicle on a public undo list for TPM to query. The TPM of the variant vehicle no longer provides the signature key and new pseudonym for the vehicle after checking the TPM revocation list.

1. If the cluster head finds a mutated vehicle, it calculates a series of $alert_i = sk_{head} + r_{i,2} \cdot H_3(sig_{j,2} \parallel M_{j,2})P_{pub}$, where j is less than the number of all the members in the cluster, $alert_0$ represents the mutated vehicle and the rest represent other ordinary vehicles in the cluster. Then the cluster head sends $(U_{head}, alert_i, AID_{head,1}, AID_{head,2}, sig_{j,2}, M_{j,2})$ to RSU.
2. RSU chooses a random number r_3 and computes $\alpha = e(pk_R, r_3 P)$, $c = H_4(\alpha \parallel sig_{mutate,2} \parallel M_{mutate,2})$, $S = c \cdot sk_R + r_3 \cdot pk_R$.
3. The RSU sends the (c, S) as the generated digital signature to the TA.
4. TA receives the message $(sig_{mutate,2}, M_{mutate,2})$ and signature (c, S), then first checks whether TS is fresh. If not, the message is rejected and the algorithm aborts.
5. TA computes $\alpha' = e(S, P)e(pk_R, -cP_{pub})$, $c' = H_4(\alpha', sig_{mutate,2}, M_{mutate,2})$.
6. If $c = c'$, TA computes $ID = AID_{i,2} \oplus H_1(x \cdot AID_{i,1})$, and then records ID on the revocation list.
7. The TPM on the mutated vehicle will no longer update the pseudonym and signature key for the vehicle after checking the ID of the vehicle in the revocation list.

The correctness of the α' is

$$\begin{aligned} \alpha' &= e(S, P)e(pk_R, -cP_{pub}) \\ &= e((x \cdot c + r_3)pk_R, P)e(pk_R, -x \cdot cP) \\ &= e(pk_R, P)^{x \cdot c + r_3 - x \cdot c} \\ &= e(pk_R, r_3 P) = \alpha \end{aligned} . \quad (5)$$

5. Security Analysis

In this section, we first analyze the security of the protocol, and then prove that the solution satisfies the expectations we mentioned in Section 3.

5.1. The Security of Message Authentication

Theorem 1. *This scheme is secure against forge ability under adaptive chosen message attack in the random oracle model only if the CDH problem is hard.*

Proof. Given a random instance (P, aP, bP) of CDH problem, the challenger $\mathcal{C}$ interacts with the adversary $\mathcal{A}$. In order to solve the CDH problem through $\mathcal{A}$, $\mathcal{C}$ needs to respond to $\mathcal{A}$ through random oracle.

1. *Initialization*: The challenger $\mathcal{C}$ executes the setup algorithm by inputting the security parameter ℓ to generate system parameters and sets $P_{pub} = aP$, then $\mathcal{C}$ sends params to $\mathcal{A}$. $\mathcal{C}$ maintains list H_1^{list} which are empty at first. The adversary $\mathcal{A}$ makes the following queries to $\mathcal{C}$:
2. *vehicle-private-key queries*: $\mathcal{C}$ maintains the $H_1^{list} = (AID_i, pk_{vi}, sk_{vi}, t_i)$, $\mathcal{A}$ makes a query on (AID_i, pk_{vi}), $\mathcal{C}$ executes the following operations:
if $AID_i \neq AID^*$, $\mathcal{C}$ executes H_1 query, if the H_1^{list} includes (AID_i, pk_{vi}), $\mathcal{C}$ returns pk_{vi}, sk_{vi} to $\mathcal{A}$, else $\mathcal{C}$ selects a random $t_i \in \mathbb{Z}_q^*$, returns $pk_{vi} = t_i \cdot P, sk_{vi} = t_i \cdot P_{pub}$ to the adversary and inserts $(AID_i, pk_{vi}, sk_{vi}, k_i)$ to H_1^{list}.
if $AID_i = AID^*$, $\mathcal{C}$ selects a random t_i^* and computes $pk_{vi}^* = t_i^* bP$, then $\mathcal{C}$ inserts $(PID_i^*, pk_{vi}^*, \perp, t_i^*)$ to H_1^{list}.
3. *sign queries*: The adversary can adaptively ask a signature on message m_i under identity AID_i, $\mathcal{C}$ executes the following operations:
if $AID_i \neq AID^*$, $\mathcal{C}$ looks up H_1^{list} to get sk_{vi} of AID_i and picks random $r_i, c_i \in \mathbb{Z}_q^*$, computes $U_i = r_i P$, $sig = sk_{vi} + r_i c_i P_{pub}$. (U_i, sig) as the signature on m_i under identity AID_i.
if $AID_i = AID^*$, $\mathcal{C}$ selects $c_i, r \in \mathbb{Z}_q^*$ and computes $r_i* = r - \frac{t_i b}{c_i}$, $U_i^* = r_i^* P$, $sig^* = rc_i P_{pub}$ as the signature on m_i under identity AID^*. We can verify this signature:

$$\begin{aligned} e(P, sig_i) &= e(P, rc_i P_{pub}) \\ &= e(P, rc_i P_{pub} + sk_{vi}^* - sk_{vi}^*) \\ &= e(P, rc_i P_{pub} + t_i^* abP - t_i^* abP) \\ &= e(P, ci(r - \frac{t_i^* b}{c_i}) P_{pub} + t_i^* abP) \\ &= e(P_{pub}, pk_{vi}^* + c_i U_i^*) \end{aligned}. \quad (6)$$

4. *signature forgery*: The adversary $\mathcal{A}$ outputs a signature on message m_i under the pseudonym PID^* which has never queried before. We assume that $\mathcal{A}$ makes two valid signatures $sig_1^* = sk_{v1}^* + r^* c^* P_{pub}$, $sig_2^* = sk_{v2}^* + r^* c^* P_{pub}$, where $sk_{v1} = t_1 abP$, $sk_{v2} = t_2 abP$, $U^* = r^* P$, $c^* = H_2(AID^*, m*, U^*)$. Then $\mathcal{C}$ could computes the result of the CDH problem by forking lemma [36], $abP = (sig_1 - sig_2) \cdot (t_1 - t_2)^{-1}$.

The instance of $\mathcal{C}$ solving the CDH problem can be transformed into the following three incidents:

- E_1: $\mathcal{C}$ doesn't halt the game.
- E_2: $\mathcal{A}$ forges a valid signature.
- E_2: E_2 happens and $AID_i = AID^*$.

In the above incidents happen, $\mathcal{C}$ wins the game and the probability is $\Pr[E_1 \wedge E_2 \wedge E_3]$ = $\Pr[E_1]\Pr[E_2 \mid E_1]\Pr[E_3 \mid E_1 \wedge E_2]$. According to the definition of the game, we have:

$$\begin{aligned} &\Pr[E_1] \geq (1 - \tfrac{1}{q_{skv}})^{q_{skv}}, \\ &\Pr[E_2 \mid E_1] \geq \varepsilon, \\ &\Pr[E_3 \mid E_1 \wedge E_2] \geq \tfrac{1}{q_{skv}}. \end{aligned}$$

Then, we can obtain

$$\Pr[E_1 \wedge E_2 \wedge E_3] \geq \varepsilon \cdot \frac{1}{q_{skv}} (1 - \frac{1}{q_{skv}})^{q_{skv}} \quad (7)$$

□

When q_{skv} is infinite, $\Pr[E_1 \wedge E_2 \wedge E_3]$ is negligible, so our scheme is secure. The proof of batch verification is similar to the above, and will not be repeated here.

5.2. Resist Attack

Then, we show that our proposed protocol satisfies the following security requirements.

Resilient to Replay Attack: Every message U_i,$sig_{i,1}$,$M_{i,1}$ or sig_2,M_2 sent by vehicle i is attached with a $TS1$. The receiver checks the freshness of the received message by checking whether the equation $|TS2 - TS1|$ is within an acceptable range. If an adversary intercepts a valid message with $TS1$ and broadcasts this message with a new timestamp $TS1'$, then the message will fail to pass the signature verification because of the verification mechanism. So our scheme can resist replay attack.

Resilient to Masquerade Attack: If an adversary broadcasts a malicious message as someone else (i.e. replaces his own pseudonym PID_i with someone else's pseudonym PID_i^*), the message will fail to pass the check because of the signature verification mechanism.

Resilient to Message Modification Attack: The secure traffic message is hidden in a signature $sig_{i,1}$ or $sig_{i,2}$ sent by a vehicle i, and the message $M_{i,1}$ or $M_{i,2}$ is secured by signature $sig_{i,1}$ or $sig_{i,2}$. Therefor, our scheme can effectively resist modification attack.

Resilient to Linkability Attack: Every message sent by vehicle i is identified by $AID_{i,1} = r_{i,1} \cdot P$, $AID_{i,2} = ID_v \oplus H_1(x \cdot AID_{i,1})$. For other entities except TA, $AID_{i,1}$ and $AID_{i,2}$ are two one-time pad since ID_v and $r_{i,1}$ are both unknown, so that the vehicle's real identity is private for other entities except TA.

6. Experimental Results and Analysis

To analyze the performance, we first compare this scheme's security objectives and functions with some other relevant schemes. Then we select two representative schemes and reproduce them to compare the computational costs of our scheme with the other two schemes. Finally, we use the Euclidean distance algorithm to calculate the fit of the information to ensure its authenticity of the information, use the normalization method to preprocess the data, and find the appropriate weights and thresholds to distinguish between real information and false information.

6.1. Security Comparisons

We compare the security achieved by this scheme with the existing related schemes. Suppose SG-1, SG-2, SG-3, SG-4, SG-5, and SG-6 respectively represent message authentication and integrity, identity privacy protection, unlinkability, batch verification, resistance to replay attacks, and message reliability. The comparison result is shown in Table 3.

Table 3. Feature Comparison.

Scheme	SG-1	SG-2	SG-3	SG-4	SG-5	SG-6
[10]	✓	✓	✓	✗	✓	✗
[23]	✓	✓	✗	✗	✓	✓
[37]	✓	✗	✗	✓	✓	✗
[38]	✓	✓	✓	✓	✗	✗
T-CPPA	✓	✓	✓	✓	✓	✓

According to Table 3, we can find that no solution can fully meet the goals and functions listed in the IoV. Among the related schemes compared, only our scheme and the scheme in [23] realize the authentication of message reliability, but the realization method is different. Scheme [23] uses the concept of SioV to ensure the reliability of the message, and we use the message similarity algorithm between the two to judge the reliability of the message, so that less time is consumed, and the number of communication rounds is reduced. Although a batch verification method is proposed in the scheme [10], the verification fails because the aggregated data is not simply added during verification. Therefore, we think the scheme cannot satisfy batch verification.

6.2. Computation Overhead Comparisons

We choose the Charm Crypto cryptographic library for pairing based on the Python platform, our hardware platform uses the Lenovo Xiaoxin pro14 of the Windows 11 operating system as the host machine, and the processor is 11th Gen Intel(R) Core(TM) i5-11320H @ 3.20 GHz 3.19 GHz with 16 GB of RAM. In particular, we use a virtual machine based on VMWare as the simulation environment, with a 4-core CPU, 8 GB memory, and Ubuntu 20.04 with x86_64 Linux 5.11.0-43-generic kernel as the operating system.

As shown in Figure 5, by comparing this scheme with the scheme in [10,20] in the time consumption of single signature and single verification, we find that the time consumption of our scheme is better than scheme [20] and worse than scheme [10], but scheme [10] has limitations in batch verification, so overall our scheme is better.

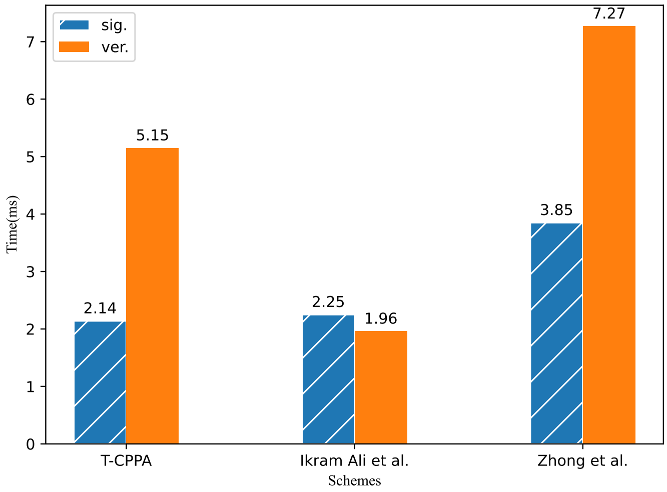

Figure 5. Computation costs of message signature and single verification stages.

Because we have analyzed the scheme [10] before making errors in batch verification, here we only compare the efficiency of batch verification with the scheme [20]. As shown in Figure 6, when the number of messages increases, the verification time increases accordingly, and the time consumption of our scheme is optimal under the same number of messages.

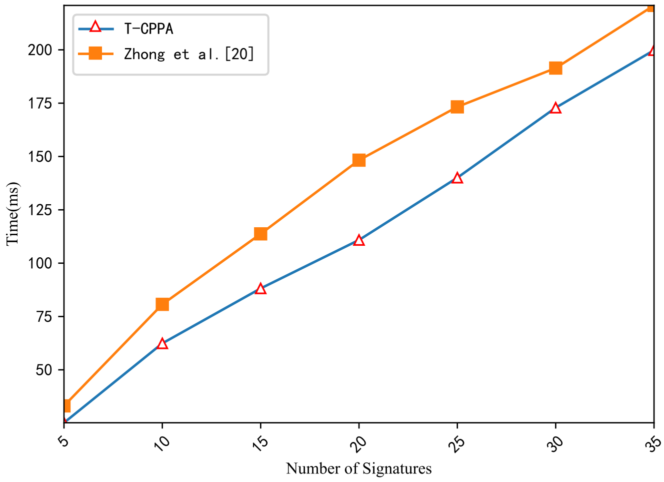

Figure 6. Computation costs of the batch verification stage.

Therefore, we can conclude that our scheme has better advantages than other schemes in terms of time consumption when signing and verifying messages. According to the actual situation, the number of vehicles in the cluster does not exceed 35, and the delay of calculating batch verification will not have a significant impact on the entire system. It is suitable for VANETs with high real-time requirements.

6.3. Message Authenticity

Dataset Description: We perform a simple simulation of the road condition information sent by the vehicle. This information includes: the vehicle's speed, coordinates, and the degree of road congestion. There are four levels of congestion, namely, open, slight congestion, severe congestion, and accident. Then we quantified the degree of congestion as 1, 2, 3, 4.

Normalization: After processing a piece of information, we get an n-dimensional vector. Different features represent different meanings with various dimensional values. We need to normalize all the features in the dataset. Here, we use the most commonly Min-Max scaling method. The feature X is normalized according to the following formula:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - Xmin} \tag{8}$$

where X_{max}, X_{min} are the maximum and minimum values in the original dataset.

Feature Value Weighting: Each dimension of the feature vector is not equally important when judging the authenticity of the message. Combined with the actual situation, it can be known that the location of the vehicle will affect the vehicle's judgment of the degree of congestion, which directly leads to the difference in the similarity of the information. In order to better obtain the degree of similarity between the information, we weigh the importance of road condition judgments according to each feature in real life. As in the previous article, the total weight of each dimension is 1. Here, we set the weight of the vehicle speed to 0.15, the weight of the coordinates to 0.05 and 0.15, and the weight of the degree of congestion to 0.65.

As shown in Figures 7 and 8, we can see the changes in the data after unweighting and adding weights and finding a suitable threshold to distinguish malicious nodes. Note that this solution only makes a simple assumption on actual examples, and focuses more on providing a reasonable idea and a solution for subsequent research.

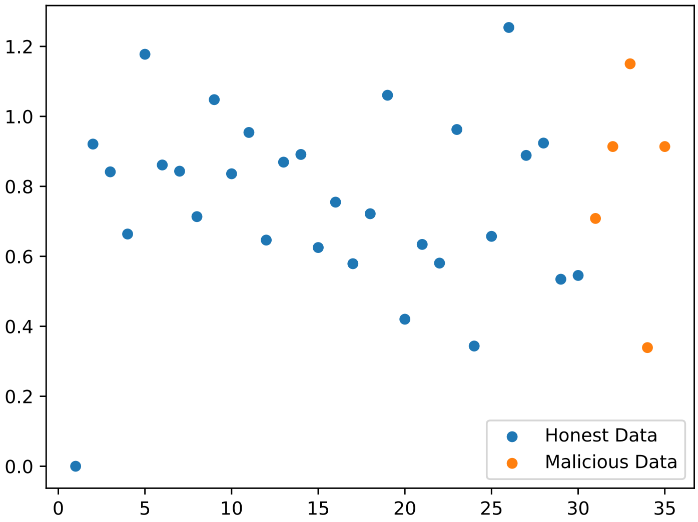

Figure 7. Unweighted data distribution.

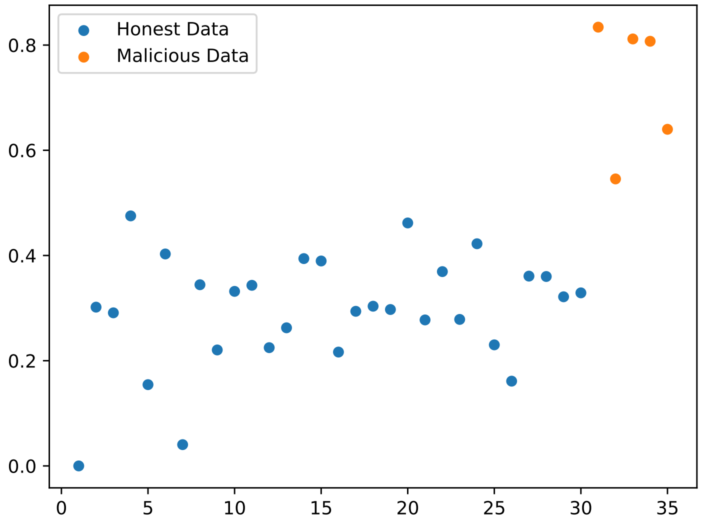

Figure 8. Weighted data distribution.

7. Conclusions

We have designed an effective identity-based signature scheme, using bilinear mapping to accelerate the process of authentication of messages by entities in VANETs. Our solution uses a batch signature verification method, allowing the receiver to authenticate extensive traffic-related messages from different vehicles in an environment with high traffic density. In addition, with the advantage of the cluster-based model, we propose a method that can detect malicious messages in real-time and improve the system's fault tolerance. This scheme can effectively protect the vehicle's privacy, and the TA can track the specific vehicle to achieve conditional privacy preservation. It can also resist various attacks, such as replay attacks, modification attacks, and forgery attacks. In terms of computing overhead, performance analysis shows that the computing overhead of our solution has also achieved a considerable performance.

For future work, we plan to apply the scheme in practical scenarios and test the impact of vehicles on network delay and packet loss rate at different speeds through a network simulation platform.

Author Contributions: Conceptualization, M.Z., B.Z. and Y.L.; methodology, M.Z. and Y.L.; software, B.Z.; validation, Y.W.; formal analysis, Y.W.; investigation, Y.W.; resources, B.Z.; data curation, B.Z.; writing—original draft preparation, B.Z.; writing—review and editing, Y.W and Y.L.; visualization, B.Z.; supervision, M.Z. and Y.W.; project administration, M.Z.; funding acquisition, M.Z. 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 62072134, U2001205, and the Key Research and Development Program of Hubei Province under Grant 2021BEA163.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Su, Y.; Shen, G.; Zhang, M. A novel privacy-preserving authentication scheme for v2g networks. *IEEE Syst. J.* **2019**, *14*, 1963–1971. [CrossRef]
2. 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]

3. Soleymani, S.A.; Abdullah, A.H.; Hassan, W.H.; Anisi, M.H.; Goudarzi, S.; Baee, M.A.R.; Mandala, S. Trust management in vehicular ad hoc network: A systematic review. *EURASIP J. Wirel. Commun. Netw.* **2015**, *2015*, 1–22. [CrossRef]
4. Hussain, R.; Lee, J.; Zeadally, S. Trust in vanet: A survey of current solutions and future research opportunities. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 2553–2571. [CrossRef]
5. Obaidat, M.; Khodjaeva, M.; Holst, J.; Zid, M.B. *Security and Privacy Challenges in Vehicular Ad Hoc Networks*; Springer International Publishing: Cham, Switzerland, 2020; pp. 223–251.
6. Alshudukhi, J.S.; Mohammed, B.A.; Al-Mekhlafi, Z.G. Conditional privacy-preserving authentication scheme without using point multiplication operations based on elliptic curve cryptography (ecc). *IEEE Access* **2020**, *8*, 222032–222040. [CrossRef]
7. Jo, H.J.; Kim, I.S.; Lee, D.H. Reliable cooperative authentication for vehicular networks. *IEEE Trans. Intell. Transp. Syst.* **2017**, *19*, 1065–1079. [CrossRef]
8. Wang, Y.; Zhong, H.; Xu, Y.; Cui, J.; Wu, G. Enhanced security identity-based privacy-preserving authentication scheme supporting revocation for vanets. *IEEE Syst. J.* **2020**, *14*, 5373–5383. [CrossRef]
9. Zhang, M.; Song, W.; Zhang, J. A secure clinical diagnosis with privacy-preserving multi-class support vector machine. *IEEE Syst. J.* **2022**, *16*, 67–78. [CrossRef]
10. Ali, I.; Li, F. An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in vanets. *Veh. Commun.* **2020**, *22*, 100228. [CrossRef]
11. Gurung, S.; Lin, D.; Squicciarini, A.; Bertino, E. Information-oriented trustworthiness evaluation in vehicular ad-hoc networks. In Proceedings of the International Conference on Network and System Security, Madrid, Spain, 3–4 June 2013; Springer: Berlin/Heidelberg, Germany, 2013; pp. 94–108.
12. Kerrache, C.A.; Calafate, C.T.; Cano, J.-C.; Lagraa, N.; Manzoni, P. Trust management for vehicular networks: An adversary-oriented overview. *IEEE Access* **2016**, *4*, 9293–9307. [CrossRef]
13. Yao, X.; Zhang, X.; Ning, H.; Li, P. Using trust model to ensure reliable data acquisition in vanets. *Ad Hoc Netw.* **2017**, *55*, 107–118. [CrossRef]
14. Kerrache, C.A.; Lagraa, N.; Hussain, R.; Ahmed, S.H.; Benslimane, A.; Calafate, C.T.; Cano, J.-C.; Vegni, A.M. Tacashi: Trust-aware communication architecture for social internet of vehicles. *IEEE Internet Things J.* **2018**, *6*, 5870–5877. [CrossRef]
15. Ghaleb, F.A.; Maarof, M.A.; Zainal, A.; Al-Rimy, B.A.S.; Saeed, F.; Al-Hadhrami, T. Hybrid and multifaceted context-aware misbehavior detection model for vehicular ad hoc network. *IEEE Access* **2019**, *7*, 159119–159140. [CrossRef]
16. Song, L.; Sun, G.; Yu, H.; Du, X.; Guizani, M. Fbia: A fog-based identity authentication scheme for privacy preservation in internet of vehicles. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5403–5415. [CrossRef]
17. Raya, M.; Hubaux, J.-P. Securing vehicular ad hoc networks. *J. Comput. Secur.* **2007**, *15*, 39–68. [CrossRef]
18. Lin, J.; Jing, J.; Zhang, Q.; Wang, Z. Recent advances in pki technologies. *J. Cryptologic Res.* **2015**, *2*, 487C496.
19. Asghar, M.; Doss, R.R.M.; Pan, L. A scalable and efficient pki based authentication protocol for vanets. In Proceedings of the 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), Sydney, Australia, 21–23 November 2018; IEEE: Piscataway, NJ, USA , 2018; pp. 1–3.
20. Zhong, H.; Han, S.; Cui, J.; Zhang, J.; Xu, Y. Privacy-preserving authentication scheme with full aggregation in vanet. *Inf. Sci.* **2019**, *476*, 211–221. [CrossRef]
21. Xiong, W.; Wang, R.; Wang, Y.; Zhou, F.; Luo, X. Cppa-d: Efficient conditional privacy-preserving authentication scheme with double-insurance in vanets. *IEEE Trans. Veh. Technol.* **2021**, *70*, 3456–3468. [CrossRef]
22. Wei, F.; Zeadally, S.; Vijayakumar, P.; Kumar, N.; He, D. An intelligent terminal based privacy-preserving multi-modal implicit authentication protocol for internet of connected vehicles. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 3939–3951. [CrossRef]
23. Liu, Y.; Wang, Y.; Chang, G. Efficient privacy-preserving dual authentication and key agreement scheme for secure v2v communications in an iov paradigm. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2740–2749. [CrossRef]
24. Huang, Z.; Ruj, S.; Cavenaghi, M.A.; Stojmenovic, M.; Nayak, A. A social network approach to trust management in vanets. *Peer-To-Peer Netw. Appl.* **2014**, *7*, 229–242. [CrossRef]
25. Zhou, A.; Li, J.; Sun, Q.; Fan, C.; Lei, T.; Yang, F. A security authentication method based on trust evaluation in vanets. *EURASIP J. Wirel. Commun. Netw.* **2015**, *2015*, 1–8. [CrossRef]
26. He, D.; Chan, S.; Guizani, M. Handover authentication for mobile networks: Security and efficiency aspects. *IEEE Netw.* **2015**, *29*, 96–103. [CrossRef]
27. Wang, S.; Yao, N.; Gong, N.; Gao, Z. A trigger-based pseudonym exchange scheme for location privacy preserving in vanets. *Peer-to-Peer Netw. Appl.* **2018**, *11*, 548–560. [CrossRef]
28. Liu, J.; Li, X.; Jiang, Q.; Obaidat, M.S.; Vijayakumar, P. Bua: A blockchain-based unlinkable authentication in vanets. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; IEEE: Piscataway, NJ, USA , 2020; pp. 1–6.
29. Tzeng, S.-F.; Horng, S.-J.; Li, T.; Wang, X.; Huang, P.-H.; Khan, M.K. Enhancing security and privacy for identity-based batch verification scheme in vanets. *IEEE Trans. Veh. Technol.* **2015**, *66*, 3235–3248. [CrossRef]
30. Sun, X.; Lin, X.; Ho, P.-H. Secure vehicular communications based on group signature and id-based signature scheme. In Proceedings of the 2007 IEEE International Conference on Communications, Glasgow, UK, 24–28 June 2020; IEEE: Piscataway, NJ, USA, 2007; pp. 1539–1545.

31. 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; IEEE: Piscataway, NJ, USA, 2007; pp. 103–108.
32. Lu, R.; Lin, X.; Liang, X.; Shen, X. A dynamic privacy-preserving key management scheme for location-based services in vanets. *IEEE Trans. Intell. Transp. Syst.* **2011**, *13*, 127–139. [CrossRef]
33. Zhang, M.; Zhang, Y.; Shen, G. Ppdds: A privacy-preserving disease diagnosis scheme based on the secure mahalanobis distance evaluation model. *IEEE Syst. J.* **2021**, 1–11. [CrossRef]
34. Zhang, M.; Chen, Y.; Lin, J. A privacy-preserving optimization of neighborhood-based recommendation for medical-aided diagnosis and treatment. *IEEE Internet Things J.* **2021**, *8*, 10830–10842. [CrossRef]
35. Wikipedia Contributors, Trusted Platform Module—Wikipedia, the Free Encyclopedia. 2022. Available online: https://en.wikipedia.org/w/index.php?title=Trusted_Platform_Module&oldid=1086571731 (accessed on 9 May 2022).
36. Pointcheval, D.; Stern, J. Security proofs for signature schemes. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Zaragoza, Spain, 12–16 May 1996; Springer: Berlin/Heidelberg, Germany, 1996; pp. 387–398.
37. Li, J.; Liu, Y.; Zhang, Z.; Li, B.; Liu, H.; Cheng, J. Efficient id-based message authentication with enhanced privacy in wireless ad-hoc networks. In Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 5–8 March 2018; IEEE: Piscataway, NJ, USA , 2018; pp. 322–326.
38. Liu, J.; Yu, Y.; Zhao, Y.; Jia, J.; Wang, S. An efficient privacy preserving batch authentication scheme with deterable function for vanets. In Proceedings of the International Conference on Network and System Security, Hong Kong, China, 27–29 August 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 288–303.