PLOS ONE

RESEARCH ARTICLE

Anonymous-authentication scheme based on fog computing for VANET

Mu Han[1], **Shuai Liu**[1], **Shidian Ma**[2]*, **Ailan Wan**[1]

1 School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang, China,
2 Automotive Engineering Research Institute Jiangsu University, Zhenjiang, China

* hanmuktz888@gmail.com

Check for updates

OPEN ACCESS

Citation: Han M, Liu S, Ma S, Wan A (2020) Anonymous-authentication scheme based on fog computing for VANET. PLoS ONE 15(2): e0228319. https://doi.org/10.1371/journal.pone.0228319

Editor: He Debiao, Wuhan University, CHINA

Received: October 9, 2019

Accepted: January 13, 2020

Published: February 13, 2020

Copyright: © 2020 Han et al. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Data Availability Statement: All relevant data are within the paper and its Supporting Information files.

Funding: This research is supported by the following funds: Natural Science Fund for Colleges and Universities in Jiangsu Province (12KJD580002); Jiangsu Graduate Innovation Fund (KYLX_1057); Key Research and Development Plan of Jiangsu province in 2017 (Industry Foresight and Generic Key Technology) (BE2017035) to MH. This research was also supported by the Project of Jiangsu University Senior Talents Fund (1281170019).

Abstract

Privacy protection in vehicular ad hoc networks (VANETs) has always been a research hotspot, especially the issue of vehicle authentication, which is critical to ensure the safe communication of vehicles. However, using the real identity in the process of authentication can easily result in a leak of the privacy information of the vehicles. Therefore, most existing privacy-protection schemes use anonymous authentication and require one-to-one communication between vehicles and the trusted authority (TA). However, when the number of vehicles is too large, network congestion can take place. In addition, the process of updating the anonymous by the TA or the vehicle itself, can result in both poor real-time performance and leakage of the system master key. To solve these problems, this study proposes a fog-computing-based anonymous-authentication scheme for VANETs; the scheme reduces the communication burden of the TA by enabling self-authentication between vehicles and road-side units (RSUs), thus improving the vehicle-authentication efficiency. For updating the anonymous, we design a fog-computing-based pseudonym-updating and -tracking strategy, which guarantees real-time communication and reduces the instances of re-authentication interactions for legitimate vehicles. The experimental results show that the scheme not only meets the privacy-protection requirements of VANETs but also offers better performance than that of the existing anonymous-authentication schemes.

Introduction

The vehicular ad hoc network (VANET) is a core component of the intelligent transportation system and plays an indispensable role in many aspects such as improving communication efficiency and reducing traffic accidents [1]. The nodes of VANET comprise the following two parts: the onboard unit (OBU), which is installed in vehicles and the road-side unit (RSU), which is located on the road-side [2]. Using the OBU, vehicles can achieve the vehicle-to-vehicle, vehicle-to-infrastructure, and broadcast communications [3] for comfortable and safe services (e.g., weather information, entertainment-related internet service, and traffic accidents) [4]. However, owing to the characteristics of the open network environment and dynamic network topology, the VANET faces many challenges in the field of secure communication. As the precondition of secure communication, the authentication of vehicles guarantees the

Competing interests: The authors have declared that no competing interests exist.

legitimacy of each communication node for vehicles to achieve secure communication. Therefore, the authentication of vehicles is particularly important in the VANET. However, there are still some challenges: 1) how to implement an efficient and secure authentication scheme between the vehicles and RSU [5]; 2) how to protect the privacy of users during the process of authentication. Therefore, designing an efficient and secure anonymous-authentication scheme has wide applications [6–7].

In recent years, researchers have proposed many authentication schemes for VANET in order to address this problem. Most of these schemes achieved security authentication based on anonymous. Meanwhile, to avoid tracking attacks, vehicles need to change their pseudonyms frequently. At the beginning, these existing schemes can verify the identities of vehicles in the VANET, by which malicious vehicles could be prevented from communicating with other legitimate vehicles or RSUs, and, thus, the privacy information of the vehicles could also be protected. However, it is difficult to accomplish efficient authentication when the number of authentication requests increases in a short time, and if the certificate revocation list (CRL) is large. Subsequently, the transmission delay gets longer when the size of the CRL becomes larger [8]. During this period, malicious vehicles can continually compromise the VANET. Also, broadcasting the CRL to other vehicles will disclose the privacy information of the revocation vehicles, as the legal vehicles have all the pseudonyms of the revoked vehicles. Considering the issues of inefficient authentication and costs caused by the CRL, many related scholars proposed several efficient authentication schemes using the hash message authentication code (HMAC), which prevents the attackers from changing the content of the messages sent by legitimate vehicles or RSUs [9]. Moreover, if an anonymous vehicle in the VANET system becomes malicious, its privacy should be revoked by the trusted authority (TA) and revealed to other vehicles [10], so that it can no longer be anonymous; this is done to protect the performance of the system. Thus, the revocation scheme has been considered as very essential to retain other users as honest in the VANET [11].

In this study, we proposed a novel authentication scheme that leverages fog-computing architecture to protect the privacy of vehicles (i.e., achieving anonymity) for the VANET. The following are the main contributions of this study:

1. A two-way anonymous-authentication scheme, which is based on anonymity, is designed, in which the RSU and the vehicle do not need the TA in order to participate in the process of identity authentication, thereby reducing the burden of the trusted center, as well as the authentication delay.
2. By introducing fog computing to generate and update the anonymity of vehicles, legitimate vehicles do not need to authenticate all the RSUs in the driving period, thereby reducing the times of authentications between legitimate vehicles and RSUs.

The rest of this paper is structured as follows: Section 2 details the related work; Section 3 provides the system model; Section 4 presents the proposed scheme; Section 5 provides the security analysis of this paper. Section 6 analyses the performance of the proposed protocol. Finally, Section 7 concludes this paper.

Related work

The existing authentication schemes for the VANET are mainly based on pseudonyms in order to achieve efficient and secure anonymous authentication.

Lu et al. [12] proposed a pseudonym-based effective conditional privacy-protection protocol, which is based on bilinear mapping, to obtain the conditional privacy of vehicles. However, the RSU has high latency while generating pseudonyms. In addition, the RSU is usually

vulnerable to physical attacks and hazards, thereby not guaranteeing security very well. Huang et al. [13] proposed an efficient pseudonymous authentication-based conditional privacy protocol for VANETs (PACP), in which the TA first generates a long-term pseudonym for vehicles, following which the vehicles obtain a "token" from the RSU. Finally, the vehicles generates its own pseudonym to achieve anonymous communication. However, the limitation of PACP is that during token generation, the RSU does not know any information regarding vehicles, and it is the only entity to generate tokens in the VANET; therefore, the complete reliability of tokens cannot be guaranteed. Furthermore, Skim et al. [14] proposed a pseudonym-based conditional privacy-protection authentication protocol, which improves the efficiency of node-identity authentication by reducing the time-consuming mapping operation. However, the frequent authentication process increases not only the computation cost and authentication delay but also the burden for the authentication agency. In addition to privacy protection, how to achieve effective authentication of vehicles is also an important challenge for the contemporary VANET. Therefore, researchers proposed pseudonym-based batch authentication schemes, such as the revocable group batch authentication scheme (RGB) [15], the anonymous batch authentication and key agreement [16], and the authentication scheme for VANETs with batch verification (BVV) [17] under the random oracle model.

In addition, for designing anonymous VANET authentication scheme based on pseudonym, some papers choose group signature to achieve anonymous authentication of the node identity. Among them, Lin et al. [18] introduced group signature into the VANET for the first time, thereby preventing the leakage of the user's privacy information in the process of identity authentication. However, in the entire process, frequent group key updates increase the computational overhead; therefore, the scheme cannot meet the high efficiency requirements of the VANET. Furthermore, Zhong et al. [19] proposed an efficient group signature scheme with revocation (GSR), which combines the subset cover framework with Camenisch–Stadler. However, the group signature scheme also faces some open security problems; i.e., group administrators are not protected, and the selection of relevant vehicle group administrators may endanger the privacy of all the group members.

However, the pseudonym-based authentication scheme does not face the security threat caused by the group signature scheme, and the former is more efficient than the latter [20]. However, in the pseudonym-authentication-based VANET, one-to-one communication is required between vehicles and the TA. In addition, when the number of vehicles is too large, network congestion is caused easily. Besides, the process of anonymous update by the TA or by the vehicle itself can easily cause both poor real-time performance and leakage of the system master key.

In this study, we provide a fog-computing-based anonymous-authentication scheme for the VANET; the scheme reduces the communication burden of the TA by performing self-authentication between vehicle and RSUs, thereby improving the efficiency of vehicle authentication. For an anonymous update, we design a fog-computing-based pseudonym-updating and tracking strategy, which guarantees real-time communication and reduces the instances of re-authentication interactions for legitimate vehicles.

System overview

System model

The system model of this study is depicted in Fig 1, which consists of three major layers, namely, the cloud layer, the fog layer, and vehicles.

1. Cloud layer: It is the trust authority of the entire system and has the powerful ability to calculate and store a large amount of information. Clouds mainly include the TA, computing

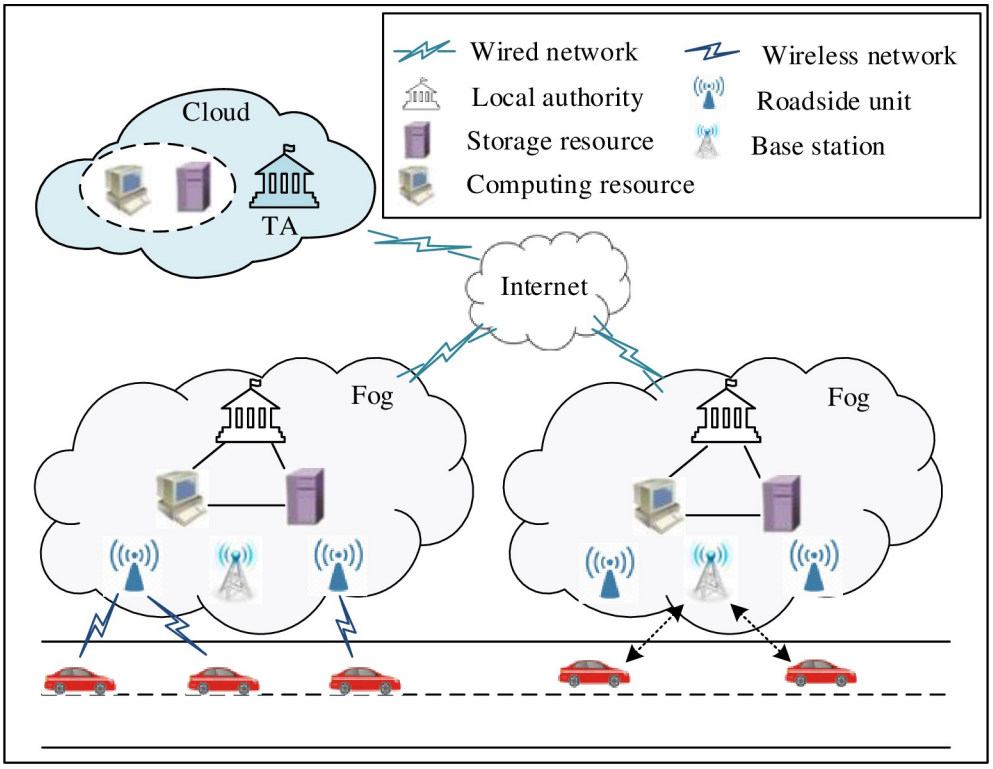

Fig 1. Network model.

https://doi.org/10.1371/journal.pone.0228319.g001

resources, and storage resources. In this study, first, the TA is responsible for registering and managing the local authorities (Las) and vehicles, as well as allocating certification and system parameters to them simultaneously. Second, it also exposes the true identities (TIDs) of the vehicles in a traffic dispute.

2. Fog layer: In cloud computing, the elements of the network infrastructure (such as RSU and base station) are deployed near the edge of the network, and they are interconnected to form a fog layer. In the network infrastructure, there is a dedicated local fog server to connect to the Internet wirelessly, and to provide a wireless interface for vehicles to access computing and storage resources. These fog servers use the network-function virtualization technology in order to virtualize the physical resources in the fog infrastructure, to build virtual machines for computing instances. In addition, to realize flexible resource allocation among fog servers, virtual machines are dynamically created, migrated, loaded, and destroyed according to different network states, by using the network technology defined by software [21]. On the basis of these technologies, the fog layer is implemented in the real scene. In this study, each fog mainly consists of five parts, namely, the LA, RSU, base station, computing resources, and storage resources. The LA is responsible for generating and updating the anonymous information of vehicles and, subsequently, recording it in the storage resources of the corresponding fog layer, thereby distributing the anonymous information to the corresponding vehicles through RSU, and, thereafter, uploading the generated anonymous information to the cloud layer. The RSU is a fixed roadside communication unit, which communicates with the LAs and vehicle through both wired and wireless networks. This study assumes that the RSU is completely trusted and is used to verify the validity of the vehicle identity, and that the anonymity generated by the LAs is forwarded to the vehicle.

3. Vehicles: Each vehicle is equipped with an OBU, which shares some value information (for example, traffic safety warnings) with RSUs and other legitimate vehicles, through wireless communication technology. Each OBU possesses a tamper-proof device for storing public keys, private keys, and other sensitive and confidential information. In addition, a global positioning system (GPS) provides the location information of vehicles.

Attack model

Owing to the openness of network environment in the VANET, it is inevitable to face the following attacks:

1. Impersonation attack: Attackers may pretend to be a legal vehicle or RSU in order to cheat other legal nodes.
2. Message repudiation attack: When the authorities reveal the real identity of the attacker, the attacker can repudiate the malicious information sent previously.
3. Error message attack: Attackers send some error messages to affect the judgment of users, which, in turn, may lead to accidents.
4. Privacy attack: Attackers obtain sensitive information of vehicles by analyzing the content of messages.
5. Message replay attack: Attackers replay valid messages that had been sent previously, to disturb transportation.

For the above-mentioned attacks, the authentication feature can resist the impersonation attack; the traceability feature can resist the message non-repudiation attack; the integrity and unforgeability features can resist the error message attack and the message replay attack; and the anonymity feature can resist the privacy attack.

Definitions and assumptions

Discrete Logarithm (DL) Problem. Let P be the generator of $\mathbb{G}_1$, for $a \in F_p^*$. Given P and aP, compute a.

The probability of $\mathcal{D}_{DL}$ success is defined as follows:

$$Adv_{DL} = \Pr[\mathcal{D}_{DL}(P, aP) = a]$$

DL Assumption: $Adv_{\mathbb{A}}^{DL}$ is a negligible value for all the PPT algorithm $\mathcal{D}_{DL}$.

Computational Diffie–Hellman (CDH) problem

Let P be the generator of $\mathbb{G}_1$, for all $a, b \in F_p^*$. Given (P, aP, bP), compute abP by using the probabilistic polynomial time algorithm $\mathbb{A}$.

The probability of $\mathbb{A}$ success is defined as follows:

$$Adv_{\mathbb{A}}^{CDH} = \Pr[\mathbb{A}(P, aP, bP) = abP : a, b \in F_p^*]$$

CDH Assumption: $Adv_{\mathbb{A}}^{CDH}$ is a negligible value for all the PPT algorithm $\mathbb{A}$.

Proposed system

As depicted in Fig 2, the main design of this system is the anonymous-authentication scheme. It includes the following two processes: system initialization, and efficient and secure authentication scheme. The summary of the symbols used in this paper is provided in Table 1.

System initialization

Cloud layer. TA: It generates the public parameters, namely, $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}, q, P, e$, and p, and initializes the system by using the following steps [22]:

1. TA chooses a random number, $\psi_{TA} \in F_q^*$, as the private key, $SK_{TA} = \psi_{TA}$, and computes the corresponding public key, $PK_{TA} = \psi_{TA}P$.
2. TA chooses hash functions $H_1 : \{0,1\} \rightarrow \mathbb{G}_1,\ h : \{0,1\} \rightarrow F_q^*$.
3. TA chooses a security symmetric cryptographic, $E_K(\cdot)$, publishes the system parameters, namely, $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}, q, P, e, p, PK_{TA}$,$H(\cdot)$,$h(\cdot)$ and $E_K(\cdot)$, following which it downloads the system parameters into fog layer and vehicles.

Fog layer. LA: The cloud layer distributes the TID, private key, public key, etc. to the LAs as follows:

1. TA chooses a random number, $\varepsilon_i \in F_p^*$, as its private key and computes the corresponding public key, $PK_{LA_i} = \varepsilon_i P$.
2. TA computes the certification parameters, $Q_{LA_i} = H(TID_{LA_i})$, $S_{LA_i} = \psi_{TA} Q_{R_i}$, following which it generates the signature, $\sigma_{SK}(PK_{LA_i}, TID_{LA_i}, L_{LA_i}, h(L_{LA_i}))$.

RSU: The cloud layer distributes the TID, private key, public key, etc. to the RSUs as follows:

1. TA chooses a random number, $\rho_i \in F_p^*$, as its private key and computes the corresponding public key, $PK_{R_i} = \rho_i P$.
2. TA computes the certification parameters, $Q_{R_i} = H(TID_{R_i})$, $S_{R_i} = \psi_{TA} Q_{R_i}$, and then generates the signature, $\sigma_{SK}(PK_{R_i}, TID_{R_i}, L_{R_i}, h(L_{R_i}))$.

Vehicles. TA distributes the pseudonym, private key, public key, etc. to the vehicles as follows:

1. TA computes the certification parameters, $Q_{V_i} = H_1(TID_{V_i})$ and $S_{V_i} = \psi_{TA} Q_{V_i}$.
2. TA chooses a random number, $r_i \in F_p^*$, as vehicles' private key, $SK_{V_i} = r_i$, then generates the public key, $PK_{V_i}^0 = r_i P$, and pseudonym, $FID_{V_i}^0 = TID_{V_i} \bigoplus H_1(r_i * PK_{TA})$, and finally generates certificates, $\sigma_{SK_{TA}}(\cdot) = \sigma_{SK_{TA}}(FID_{V_i}^0, PK_{V_i}^0)$.
3. TA sends the anonymity of vehicle V_i, $FID_{V_i}^0$, and the corresponding public key, $PK_{V_i}^0$, to the storage resource, then generates an anonymous tracking table starting with $\{FID_{V_i}^0, PK_{V_i}^0, TA\}$. The anonymous tracking table is depicted in Fig 3.

Efficient and secure authentication scheme

This study proposes an anonymous-authentication scheme, which is based on pseudonym and fog computing, to meet the efficiency and security requirements in the VANET. First, we design a self-checking authentication, instead of the traditional authentication with reliable authority, thereby improving the efficiency of illegal vehicle authentication. Furthermore, fog computing is introduced to realize anonymous management, reduce the number of authentications, and improve the efficiency of authentication.

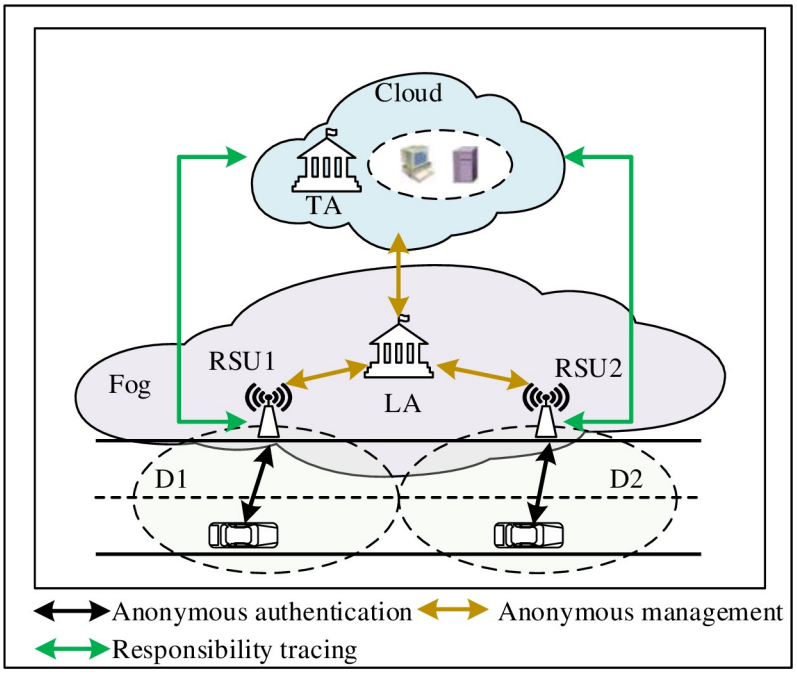

Fig 2. System design.

https://doi.org/10.1371/journal.pone.0228319.g002

In this scheme, the authentication process between the fog layer and the vehicle does not require the participation of the cloud layer. In addition, the vehicles are divided according to the following two categories: 1) Situation 1: the previous vehicles have not been certified by other RSUs in the fog layer; and 2) Situation 2: the previous vehicles have been certified by other RSUs in the fog layer. For the vehicles in Situation 1, it can be authenticated by anonymity and authentication parameters, including five information exchanges. However, in Situation 2, the vehicle can be quickly validated by checking the anonymous tracking table, requiring only two rounds of information alternation. Simultaneously, both the authentication processes can achieve anonymous authentication. The information-exchange model and both the main authentication process are depicted in Figs 4, 5 and 6, respectively. In addition, the detailed authentication process is as follows:

Table 1. Descriptions of symbols.

Symbol	Descriptions
U	Entity U, such as the vehicle or the RSU
TID_U,FID_U	True and anonymous identities of entity U
(PK_U,SK_U)	Public and private keys of entity U
Q_U,S_U	Certification parameters of entity U
$HMAC_K(\cdot)$	Hash message authentication code by using key K
$E_K(\cdot)$	Encrypt the message by using key K
$D_K(\cdot)$	Decrypt the cipher text by using key K
σ_{SK_U}	Signature of entity U
TS	Time stamp
L_U	Location of U
M_i	Message

https://doi.org/10.1371/journal.pone.0228319.t001

number	pseudonym	Public key	Generating mechanism
0	$FID_{V_i}^0$	$PK_{V_i}^0$	TA
…	…	…	…

Fig 3. Anonymous tracking table.

https://doi.org/10.1371/journal.pone.0228319.g003

RSUs broadcast the messages: RSUs broadcast messages periodically as follows:

$$M_1 : (TS, PK_{R_i}, L_{R_i}, h(L_{R_i}), \sigma_{SK_{TA}}(PK_{R_i}, L_{R_i}, h(L_{R_i}))).$$

Vehicles authenticate the RSUs. When vehicle V_i drives into the domain of RSU_i, the former could receive M_1 and verify it as follows:

- V_i receives M_1 and verifies the timestamp TS first by computing $|CT-TS|<\Delta t$, (Δt is the expected network-transmission delay).
- V_i obtains PK_{R_i}, L_{R_i}, and $h(L_{R_i})$ from M_1, and, thereafter, it verifies $\sigma_{SK_{TA}}(PK_{R_i}, L_{R_i}, h(L_{R_i}))$ by using PK_{TA}.
- V_i obtains the current geographic location, L_{V_i}, from the GPS in vehicles and, subsequently, computes $\Delta L = |L_{R_i} - L_{V_i}|$ and determines $\Delta L \leq 600$.

Upon completing the entire process, V_i completes the authentication for RSU_i.

RSUs authenticates the vehicles. Situation 1: The vehicle had not been authenticated by other RSUs previously. (see Fig 4)

- V_i selects a random number, N_1, and, thereafter, sends the message, $M_2 : (TS, E_{PK_{R_i}}(N_1, H(FID_{V_i}^0)), HMAC_{N_1}(\cdot))$, to RSU_i of the fog layer.
- RSU_i obtains N_1 from M_2 and verifies $HMAC_{N_1}(\cdot)$ first; subsequently, it selects a random number, $\alpha_i \in F_p^*$, computes $T_{R_i} = \alpha P$ and finally sends the message, $M_3 : (TS, E_{N_1}(T_{R_i}, N_1 Q_{R_i}, HMAC_{N_1}(\cdot))$, to V_i.
- V_i receives M_3 and verifies $HMAC_{N_1}(\cdot)$; subsequently, it selects a random number, $\beta_i \in F_p^*$, to compute $T_{V_i} = \beta P$ and $K_{V_i} = e(\beta N_1 Q_{R_i}, PK_{TA}) e(N_1 S_{V_i}, T_{R_i})$, following which V_i sends the message, $M_4 : (TS, E_{N_1}(FID_{V_i}^0, PK_{V_i}^0, \sigma_{SK_{TA}}(), T_{V_i}, N_1 Q_{V_i}, K_{V_i}, HMAC_{N_1}(\cdot))$, to RSU_i.
- RSU_i obtains $FID_{V_i}^0$, T_{V_i}, $PK_{V_i}^0$, $\sigma_{SK_{TA}}(\cdot)$, $N_1 Q_{V_i}$, and K_{V_i} from M_4 and, subsequently, verifies $HMAC_{N_1}(\cdot)$, following which it calculates the parameters, $K_{R_i} = \mathrm{e}(\alpha N_1 Q_{V_i}, PK_{TA}) \mathrm{e}(N_1 S_{R_i}, T_{V_i})$. If formula (1) holds, RSU_i completes the authentication for V_i. Meanwhile, the fog layer begins to provide anonymous management services. Thus,

$$K_{V_i} = K_{R_i} \tag{1}$$

When RSU_i completes the authentication of vehicle V_i, RSU_i sends the pseudonym of vehicle authentication, as well as the corresponding public key and certificate $\{FID_{V_i}^0, PK_{V_i}^0\}$ to the local authentication, LA_m, in the fog layer.

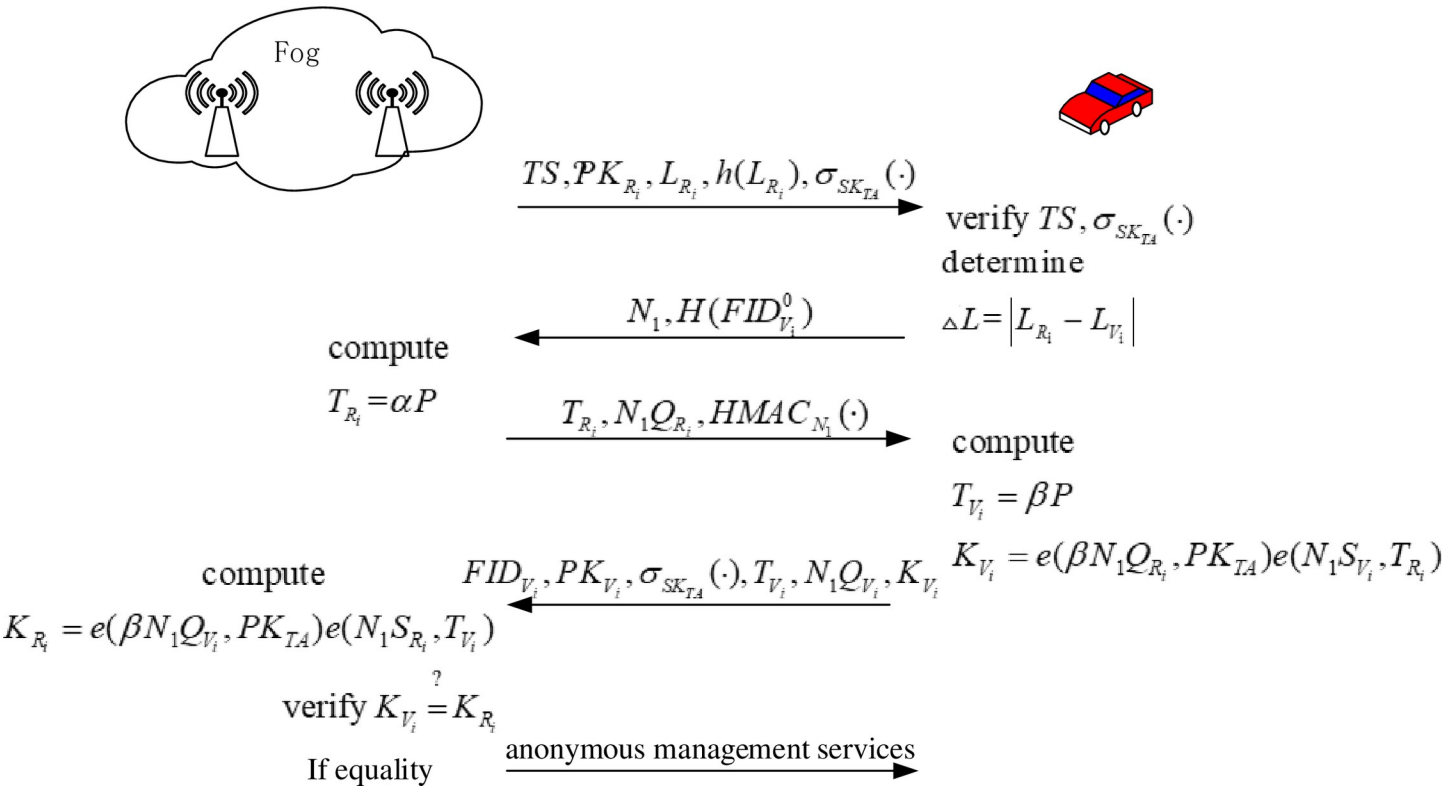

Fig 4. Authentication process for Situation 1.

https://doi.org/10.1371/journal.pone.0228319.g004

- LA_m generates w numbers of anonymities $\{FID^k_{V_i}, SK^k_{V_i}, \sigma_{SK_{LA}}(FID^k_{V_i}, PK^k_{V_i})\}^w_{k=1}$ (where $SK^k_{V_i}, \sigma_{SK_{LA}}(FID^k_{V_i}, PK^k_{V_i})$ are pseudonyms corresponding to the private key and pseudonym certificate) for vehicle V_i and, subsequently, sends them to vehicle V_i through RSU_i. Simultaneously, LA_m uploads $\{FID^k_{V_i}, PK^k_{V_i}, \sigma_{SK_{LA}}(FID^k_{V_i}, PK^k_{V_i})\}^w_{k=1}$ (see Table 2) to TA in the cloud layer.
- TA updates and stores the corresponding pseudonym tracking table of vehicles in the storage resource(the anonymous tracking table is depicted in Fig 5.), and, thereafter, sends $\{FID^k_{V_i}, PK^k_{V_i}, \sigma_{SK_{LA}}(FID^k_{V_i}, PK^k_{V_i})\}^w_{k=1}$ to the fog layer. All the RSUs in the fog layer share the updated anonymous table of vehicle V_i through fog calculation in order to reduce the authentication process of other RSUs except that of RSU_i.
- RSU updates the new anonymous table of vehicle V_i and deletes the previous anonymous table.

Situation 2: The vehicle had previously been authenticated by other RSUs. (see Fig 6)

- V_i sends the message, M_2 : $(TS,\ E_{PK_{R_i}}(FID^k_{V_i}, PK^k_{V_i}, \sigma_{SK_{LA}}(FID^k_{V_i}, PK^k_{V_i})), HMAC_{N_1}(\cdot))$, to RSU_i.
- RSU_i receives M_2, first verifies TS and $HMAC_{N_i}1(\cdot)$, and then verifies $\sigma_{SK_{LA}}(FID^k_{V_i}, PK^k_{V_i})$. If the verification is successful, the anonymous vehicle is validated according to the pseudonym tracking table sent by the TA.

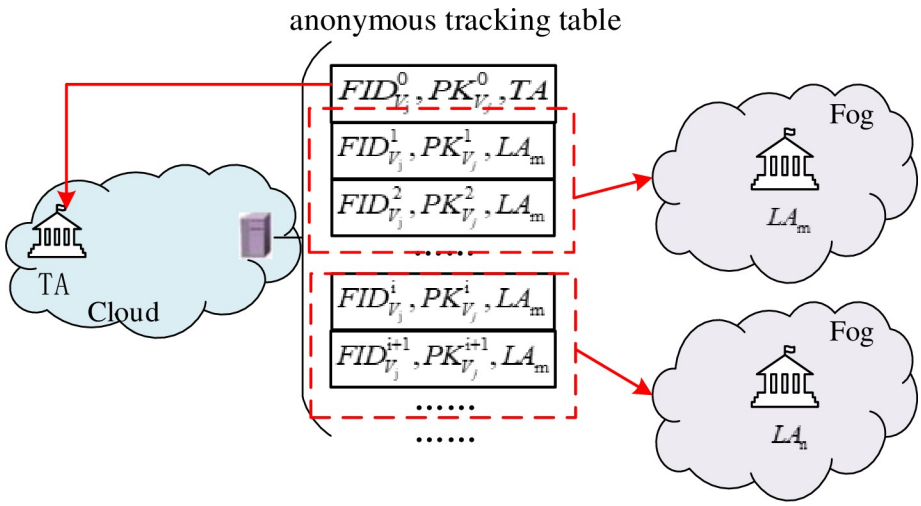

Fig 5. Corresponding pseudonym tracking table in cloud layer.

https://doi.org/10.1371/journal.pone.0228319.g005

Identity tracking

1. RSU sends the anonymous information, $\{FID_{V_j}^m, PK_{V_j}^m, \sigma_{SK_{LA}}(FID_{V_j}^m, PK_{V_j}^m)\}$ (see Fig 7), to TA in the cloud layer after discovering illegal vehicles.
2. TA finds the initial anonymity and other parameters $\{FID_{V_i}^0, PK_{V_i}^0\}$ of the illegal vehicle according to the anonymous tracking table in the storage resources.
3. Finally, TA tracks the TID of the vehicle, TID_{Vi}, by computing $TID_{V_i} = FID_{V_i}^0 \bigoplus H_1(SK_{TA} * PK_{V_i}^0)$.

Security analysis

In this section, we will provide the security analysis of this study.

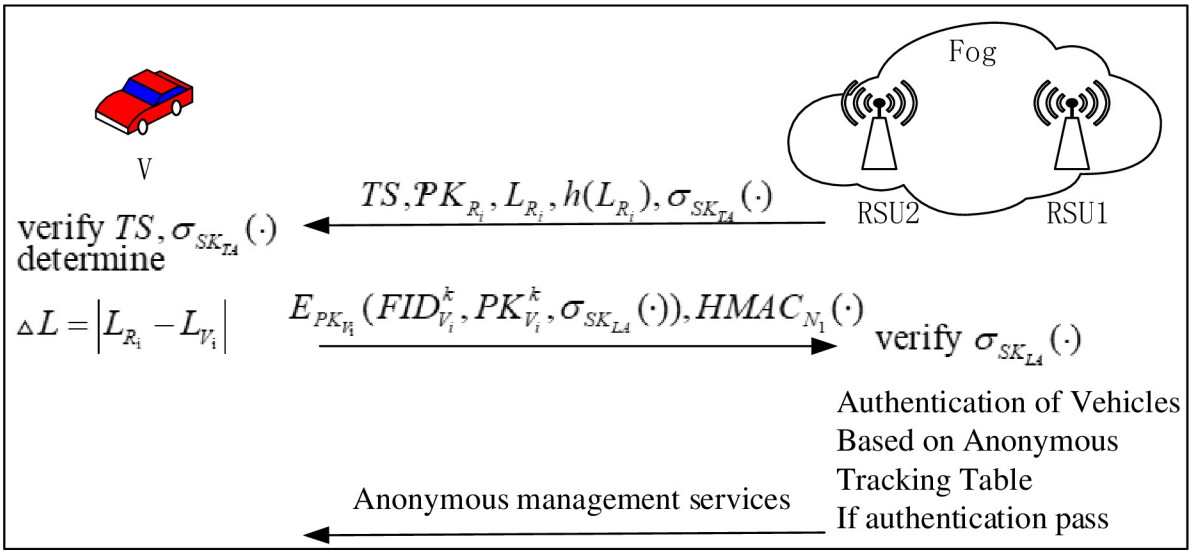

Fig 6. Authentication process for Situation 2.

https://doi.org/10.1371/journal.pone.0228319.g006

Table 2. Anonymities of vehicle V_i generated by LA_m.

Pseudonym	Public key	Generating mechanism
$FID_{V_i}^1$	$PK_{V_i}^1$	LA_m
$FID_{V_i}^2$	$PK_{V_i}^2$	LA_m
.....	.....	.....
$FID_{V_i}^k$	$PK_{V_i}^k$	LA_m
.....	.....	.....

https://doi.org/10.1371/journal.pone.0228319.t002

Authentication

The authentication of the proposed scheme is proved using the following two aspects.

Authentication of RSU. When a vehicle drive into the domain of an RSU, the former must first authenticate the identity of the latter. In this study, the authentication of the RSU is achieved by the signature and geographic location.

According to the message M_1 sent by the RSU, vehicles first verify signature $\sigma_{SK_{TA}}$, following which the vehicles compute $\Delta L = |L_{R_i} - L_{V_i}|$, and finally determine whether $\Delta L \leq 600$ to ensure the legitimacy of the RSU.

In this process, the signature $\sigma_{SK_{TA}}$ is generated by the TA, and the private key of the TA, SK_{TA}, is known only to the TA without any transmission. Therefore, any attacker cannot obtain SK_{TA} and forge the signature. Thus, only the legitimate RSU has the signature, $\sigma_{SK_{TA}}$.

In addition, the value of ΔL is calculated using the geographic location of the RSU and vehicles. If the signature, $\sigma_{SK_{TA}}$, is correct, the geographic location of the RSU, L_{R_i},in M_1 is also correct. Meanwhile, the geographic location of vehicles, L_{V_i}, is obtained from the GPS in the vehicle. Therefore, ΔL must be not be more than 600 m (the communication range of the RSU is approximately 600 m).

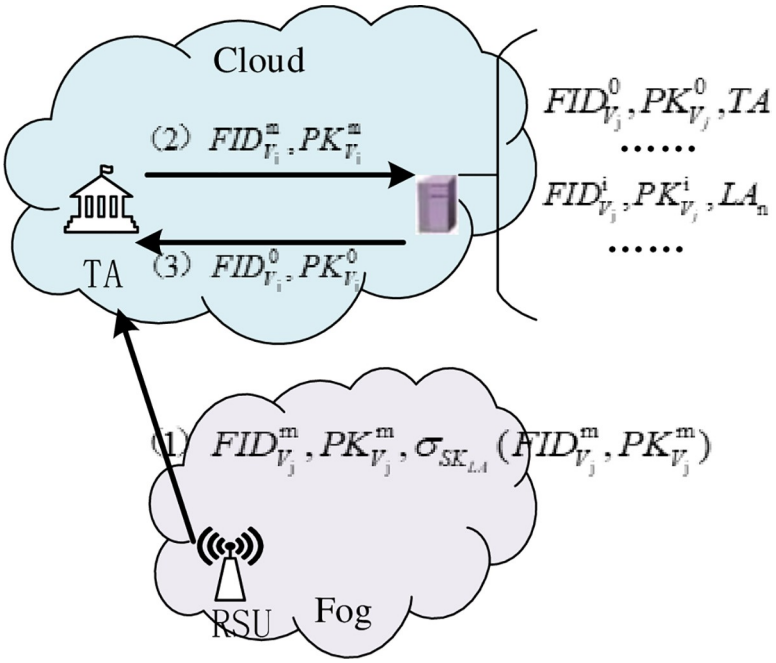

Fig 7. Identity-tracking process.

https://doi.org/10.1371/journal.pone.0228319.g007

Consequently, when $\sigma_{SK_{TA}}$ is correct and $\Delta L \leq 600$, the identity of the RSU is legal.

Authentication of vehicles.

Situation 1: The vehicle had previously been authenticated by other RSU.

If the adversary wants to impersonate a legal vehicle to get authenticated by the RSUs, it must generate a valid message, M_4, and send it to the RSUs. According to M_4, the RSUs will verify the legality of the vehicular identity on the basis of formula (2) and K_V in message, M_4. One has

$$\begin{aligned} K_V &= e(\beta N_1 Q_R, PK_{TA}) e(N_1 S_V, T_R) \\ &= e(\beta N_1 H_1(TID_R), \psi_{TA} P) e(N_1 \psi_{TA} H_1(TID_V), \alpha P) \\ &= e(\alpha N_1 H_1(TID_V) + \beta N_1 H_1(TID_R), \psi_{TA} P) \\ &= e(\alpha N_1 Q_{V_i}, PK_{TA}) \mathrm{e}(N_1 S_{R_i}, T_{V_i}) \\ &= K_{R_i} \end{aligned} \tag{2}$$

If formula (2) is workable, the identity of the vehicles is legal.

Situation 2: The vehicle had previously been authenticated by other RSUs.

If the vehicle had previously been authenticated by RSU_{i-1}, then RSU_i only needs to authenticate it according to the anonymous tracking table sent by the cloud.

Theorem: Assuming that $\mathcal{H}$ is a random oracle, the DL and CDH assumptions are valid, and the identities of the vehicles in this scheme are authenticated.

Proof: If an adversary, $\mathcal{A}$, could impersonate a real identity of a legal vehicle, TID_V, and generate a valid message, M_4, then it must be able to compute the valid value of the parameter $S_V = sP = \psi_{TA} Q_V P = \psi_{TA} H_1(TID_V) P$. The advantage of the success of $\mathcal{A}$ is $Adv_{\mathcal{A}}^{M4}$.

Constructing two algorithms, $\mathcal{D}_{CDH}$ and $\mathcal{D}_{DL}$, to solve the CDH and DL problems, respectively.

Game 1:

Setup: According to the section system initialization, $\mathcal{D}_{DL}$ generates the public parameters, namely, $\mathbb{G}_1, \mathbb{G}_2, P, q, e, \mathbb{G}, p, g,\ PK_{TA}, H_1(\cdot), h(\cdot),$ and $E_k(\cdot)$, and sends them to $\mathcal{A}$. Subsequently, $\mathcal{A}$ could query $\mathcal{D}_{DL}$ up to q_{DL} times.

Query:

1. $\mathcal{A}$ queries what is TID_V equal to?
2. $\mathcal{D}_{DL}$ defines $s = H_1(TID_V)P$ and returns it to $\mathcal{A}$.

Challenge 1:

1. After $\mathcal{A}$ received s, it inputs (P,s) to obtain $H_1(TID_V)$ by $\mathcal{D}_{DL}$;
2. $\mathcal{A}$ inputs (P,PK_{TA}) to obtain ψ_{TA};
3. $\mathcal{A}$ computes $S_V = \psi_{TA} H_1(TID_V) P$.

In the above-mentioned process, the advantage of the success of $\mathcal{A}$ is $Adv_{\mathcal{A}}^{DL} = 2q_{DL} \cdot Adv_{DL}$.

Game 2:

Setup: According to the section system initialization, $\mathcal{D}_{DL}$ generates the public parameters, $\mathbb{G}_1, \mathbb{G}_2, P, q, e, \mathbb{G}, p, g,\ PK_{TA}, H_1(\cdot), h(\cdot),$ and $E_k(\cdot)$, and sends them to $\mathcal{A}$. Thereafter, $\mathcal{A}$ could query $\mathcal{D}_{CDH}$ up to q_{CDH} times.

Query:

1. $\mathcal{A}$ queries what is TID_V equal to?
2. $\mathcal{D}_{CDH}$ defines $s = H_1(TID_V)P$ and returns it to $\mathcal{A}$.

Challenge 2:

After $\mathcal{A}$ receives s. it inputs (P, PK_{TA}, s) to obtain $H_1(TID_V)$ by $\mathcal{D}_{CDH}$.

In the above-mentioned process, the advantage of the success of $\mathcal{A}$ is $Adv_{\mathcal{A}}^{CDH} = q_{CDH} \cdot Adv_{CDH}$.

In summary, the advantage of $\mathcal{A}$ generating the valid message, M_4, i.e., the advantage of successfully calculating the valid parameter S_V is as follows:

$$\begin{aligned} Adv_{\mathcal{A}}^{M_4} &= Adv_{\mathcal{A}}^{DL} + Adv_{\mathcal{A}}^{CDH} \\ &= 2q_{DL} \cdot Adv_{DL} + q_{CDH} \cdot Adv_{CDH} \end{aligned}$$

According to the section definitions and assumptions, the advantage of $\mathcal{D}_{DL}$ successfully solving the DL problem and that of $\mathcal{D}_{CDH}$ successfully solving the CDH problem, in polynomial time, can be neglected. Thus, the advantages of $\mathcal{A}$ successfully generating a valid message, M_4, is also negligible.

Therefore, the identity of the vehicle in Situation 1 satisfies the authentication requirement of the node identity. However, if the vehicle had previously been authenticated by $RSU_{i\pm1}$ (Situation 2), then the latter only needs to authenticate the former according to the anonymous tracking table sent by the cloud.

Anonymity of vehicles

The anonymity of the proposed scheme is realized by the anonymous management of cloud and fog.

Sensitive information such as FID_{V_i} is included in the information sent by vehicles. In clouds, because the private key of the TA is secure, except for that of vehicles, only the TA knows the real identity of the vehicles; therefore, attackers cannot forge pseudonyms issued by clouds. In addition, only the TA in the cloud can reveal the relationship between vehicle anonymity and real identity, when illegal vehicles are found. In the fog layer, the RSU can authenticate the vehicle anonymously without knowing the real identity of the vehicle. Simultaneously, because the LA generates a pseudonym without obtaining the real name of the legitimate vehicle and uploads the pseudonym to the cloud, it cannot be traced back to obtain the real name of the vehicle. Therefore, no attacker can obtain the real identity of the vehicle.

Traceability

Vehicles communicate with the RSU by using their anonymities, and some malicious vehicles may send false information to cause traffic accidents. In this situation, the cloud layer can reveal the identity of the vehicles with the help of the TA and the storage resources of the cloud layer.

After receiving the anonymous, $\{FID_{V_j}^m, PK_{V_j}^m, \sigma_{SK_{LA}}(\cdot)\}$, of the irregular vehicle V sent by the RSU, the cloud finds the initial anonymous, $\{FID_{V_i}^0, PK_{V_i}^0\}$, of vehicle V in the anonymous tracking table of the storage resources. Thereafter, the initial anonymity is sent to the TA. When the TA receives $\{FID_{V_i}^0, PK_{V_i}^0\}$, it obtains the real name, TID_V, of the illegal vehicle according to the following formula:

$$\begin{aligned} TID_V &= FID_{V_i}^0 \oplus H_1(SK_{TA} * PK_{V_i}^0) \\ &= TID_{V_i} \oplus H_1(r_i * PK_{TA}) \oplus H_1(SK_{TA} * PK_{V_i}^0) \\ &= TID_{V_i} \end{aligned} \tag{3}$$

Thus, the traceability of the proposed scheme is achieved.

Message integrity and unforgeability

In the VANET, messages are more likely to become invalid requests, such as packet loss or bogus messages forged by attackers, as the communication model between the vehicles and RSU or among the vehicles, is based on wireless communication. To ensure the integrity of the messages, most existing schemes utilize HMAC or signature. In this study, the integrity of the messages can be achieved using HMAC because of its lightweight overhead.

In this study, the unforgeability of the messages is achieved by $\sigma_{SK_{TA}}$ or $HMAC_{N_1}(\cdot)$. In message M_1, the signature, $\sigma_{SK_{TA}}$, is generated by the TA by using its private key SK_{TA}. Because SK_{TA} is only held by the TA, attackers cannot compute it according to the public key $PK_{TA} = \psi_{TA}P$. Thus, $\sigma_{SK_{TA}}$ cannot be unforged by attackers. In messages M_2–M_5, N_1 is the shared key between the vehicles and RSU. Vehicles encode it using the public key of the RSU and then send it back. However, only the RSU can decode it using its private key, SK_{RSU}, and obtain N_1. Thus, attackers are unable to gain N_1 and forge messages.

Performance evaluation

In this section, we evaluate the performance of the proposed scheme. First, we compare the proposed scheme with the existing schemes in terms of computation and communication costs. In addition, we evaluated the average delay of the proposed scheme.

Computation cost analysis and comparison

According to reference [23], the computation cost mainly depends on the following three parameters: first, the time taken to execute a pairing operation, T_p; second, the time taken to execute one-point multiplication over an elliptic curve, T_m; and third, the time taken to execute a MapToPoint hash function, T_h, where T_p = 1.6 ms, T_m = 0.6 *ms* and T_h = 2.7*ms*. This paper does not consider other operations requiring low computational costs, such as the HMAC operation (executing time is 0.006 ms).

Because this study divides vehicles into two categories, both of which have has been mentioned previously, the number of vehicles needed to be verified, n, includes the number of vehicles in Situation 1, n_1, and that in Situation 2, n_2; therefore, $n = n_1+n_2$. Furthermore, Table 3 and Fig 8 objectively illustrate the comparison between our proposed scheme and other existing schemes, in terms of the verification time. From Fig 8, it can be observed that our proposed scheme requires lower computational cost. Especially, when the number of vehicles, n, is equal to 100, the CPAS, RGB, and BVV take 780.6, 968.1, and 1030 ms, respectively. Whereas the proposed scheme takes only 448 ms (n_1 = 30%n, n_2 = 70%n), or 744 ms (n_1 = 60% n,n_2 = 40%n).

Communication-cost analysis and comparison

In this paper, the communication cost is represented by the size of messages. In this section, we mainly focus on the additional communication cost, such as the cost associated with

Table 3. Verification cost of various schemes.

Scheme	Verify a vehicle	Verify n vehicles ($n = n_1+n_2$)
CPAS	$5T_m+3T_p$	$(5n+1)T_m+3nT_p$
RGB	$3T_m+T_h$	$(7n+1)T_m+(2n+1)T_h$
BVV	$3T_h+T_m+T_p$	$3nT_h+nT_m+nT_p$
Proposed	$10T_m+4T_p$ or 0	$n_1(10T_m+4T_p)+n_20$

https://doi.org/10.1371/journal.pone.0228319.t003

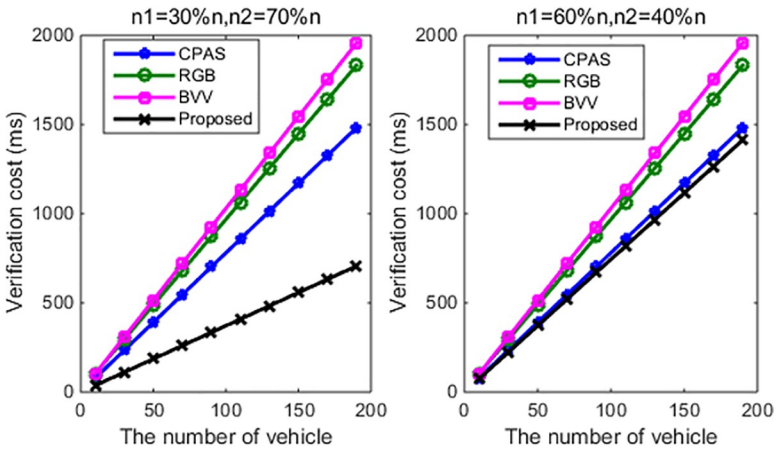

Fig 8. Number of vehicles and verification cost.

https://doi.org/10.1371/journal.pone.0228319.g008

signature, certification, and pseudonym. As shown in Table 4, the additional sizes of messages are 101 bytes for CPAS [14], 63 bytes for RGB [15], 280 bytes for BVV [17], and 76 bytes for our proposed scheme.

In addition, Fig 9 compares the communicational cost of the proposed scheme with those of some existing schemes. From the figure, we can see that the communicational cost of the proposed scheme is lower than that of each CPAS and BVV.

Experiment and simulation

To ensure the authenticity and feasibility of the experiment, the relevant parameters of this experiment are based on the real data provided by the federal government of the United States [24]. All the simulation parameters are listed in Table 5.

Average delay. This study uses formula (4) [25] for evaluating the average delay, where n denotes the number of vehicles, M_i the number of messages sent by the vehicles, $T_{creat}^{n_m}$ the time in which a vehicle or RSU creates the message m, $T_{communication}^{n_m k}$ the communication time in which the entity (vehicle or RSU) N sends the message to the entity k, and $T_{verify}^{n_m k}$ the time in which the entity k verifies the message m from the entity n. The average delays for different number of vehicles are depicted in Fig 10. One has

$$Delay_{ave} = \frac{1}{n}\sum_{i=1}^{n}\frac{1}{M_i}\sum_{m=1}^{M}(T_{creat}^{N_m} + T_{communication}^{N_{m_k}} + T_{verify}^{N_m k}) \quad (4)$$

From Fig 10, it can be clearly seen that the average delays of both the RGB and proposed scheme are less than those of the CPAS and BVV, with the same number of vehicles. In

Table 4. Comparison of communication cost.

Scheme	Send n message (bytes)
CPAS	101n
RGB	63n
BVV	280n
Proposed	76n

https://doi.org/10.1371/journal.pone.0228319.t004

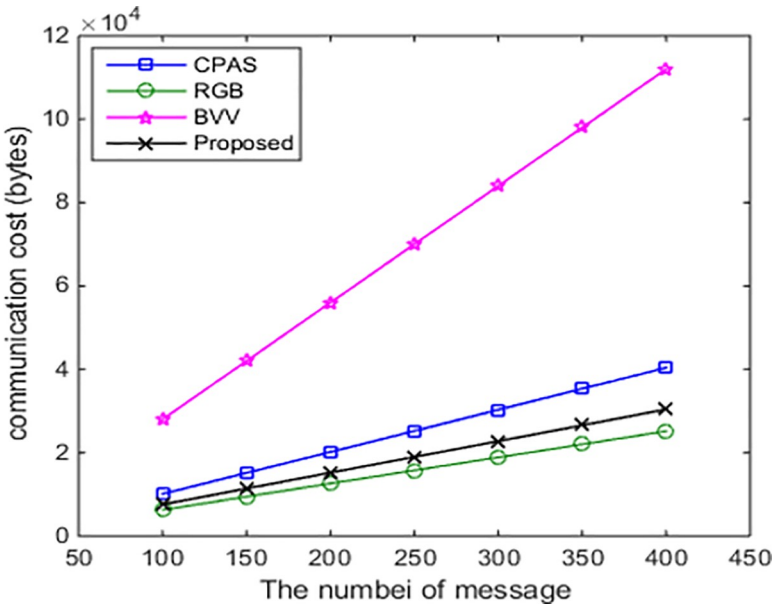

Fig 9. Number of vehicles and communication cost.

https://doi.org/10.1371/journal.pone.0228319.g009

Table 5. Simulation parameters.

Parameter	value
Simulation tool	NS2.34
Wireless protocol	802.11p
Channel bandwidth	6 Mb/s
Simulation time	30 s
Road length	1000 m
Communication range of RSU	600 m
Message size	200 bytes
Speed of vehicle	0–30 m/s

https://doi.org/10.1371/journal.pone.0228319.t005

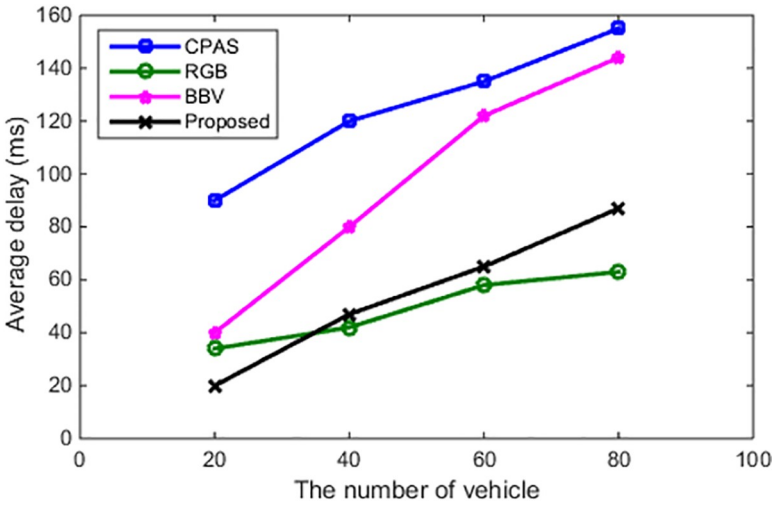

Fig 10. Number of vehicles and average delay.

https://doi.org/10.1371/journal.pone.0228319.g010

Table 6. Number of vehicles and packet-loss rate.

	Static state (%)	Dynamic state (%)
50	0.2	0.12
100	0.4	0.7
150	1.0	0.95
200	2.1	2.3

https://doi.org/10.1371/journal.pone.0228319.t006

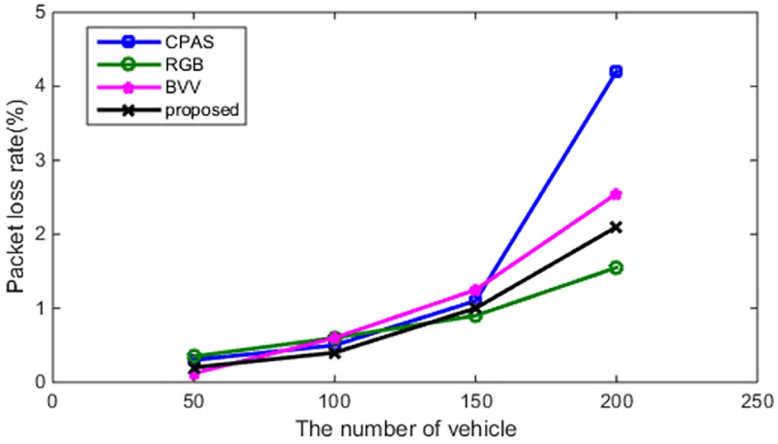

Fig 11. Number of vehicles and the packet-loss rate (static state).

https://doi.org/10.1371/journal.pone.0228319.g011

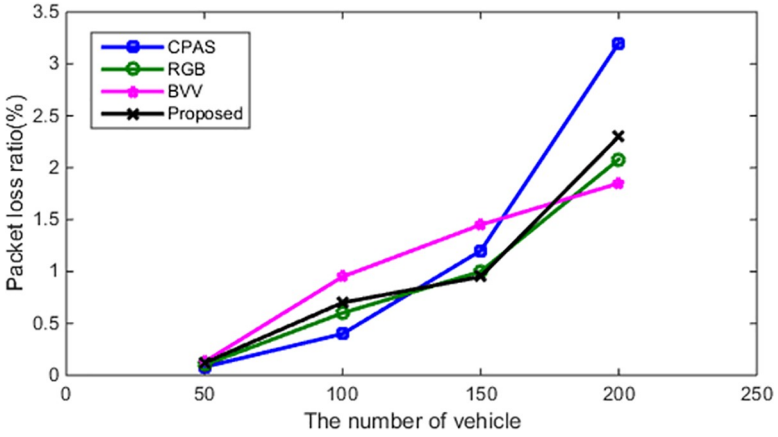

Fig 12. Number of vehicles and the packet-loss rate (dynamic state).

https://doi.org/10.1371/journal.pone.0228319.g012

addition, our proposed scheme is the most efficient of all the schemes mentioned when the number of vehicles ranges from 20 to 30. Furthermore, when the number of vehicles is more than 30, our proposed scheme becomes more efficient than CPAS and BVV as well.

Packet-loss rate. In addition to analyzing the average delay of the proposed scheme, the packet-loss rate of the proposed scheme is compared with that of various schemes, under two states, i.e., static and dynamic states (see Table 6). As depicted in Figs 11 and 12, the proposed scheme also has some advantages with respect to the packet-loss rate.

Conclusions

This study presented a fog-computing-based anonymous-authentication scheme for the VANET. In the proposed scheme, vehicles are divided according to two situations. According to the different above-mentioned situations, the RSUs in the fog layer are authenticated using pseudonyms. The pseudonym management of the vehicles is achieved via fog computing, which improves the performance after entering the first authentication, thus realizing both privacy protection and efficient authentication.

Acknowledgments

We would like to thank Editage (www.editage.com) for English language editing.

Author Contributions

Conceptualization: Shidian Ma.

Data curation: Shuai Liu.

Investigation: Ailan Wan.

Writing – original draft: Mu Han.

References

1. Pournaghi SM, Zahednejad B, Bayat M, Farjami Y. NECPPA: a novel and efficient conditional privacy-preserving authentication scheme for VANET. Comput Netw. 2018; 134, 78–92.
2. Jiang S, Zhu X, Wang L. An efficient anonymous batch authentication scheme based on hmac for vanets. IEEE Trans Intell Transp Syst. 2016; 17(8), 2193–204.
3. Cui J, Zhang J, Zhong H, Xu Y. SPACF: a secure privacy-preserving authentication scheme for vanet with cuckoo filter. IEEE Trans Veh Technol. 2017; 10283–10295.
4. Manvi SS, Tangade S. A survey on authentication schemes in vanets for secured communication. Veh Commun. 2017; 9, 19–30.
5. Whaiduzzaman M, Sookhak M, Gani A, Buyya R. A survey on vehicular cloud computing. J Netw Comput Appl. 2014; 40, 325–44.
6. Wang C, Shi D, Xu X, Fang J. An anonymous data access scheme for VANET using pseudonym-based cryptography. J Ambient Intell Humanized Comput. 2016; 7(1), 63–71.
7. Wang M, Liu D, Zhu L, Xu Y, Wang F. LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication. Computing. 2016; 98(7), 685–708.
8. Rajput U, Abbas F, Oh H. A hierarchical privacy preserving pseudonymous authentication protocol for vanet. IEEE Access. 2016; 7770–7784.
9. Ubaidullah R, Fizza A, Hasoo E, Rasheed H, Heekuck O. A two level privacy preserving pseudonymous authentication protocol for VANET. IEEE International Conference on Wireless & Mobile Computing. IEEE; 2015.
10. Shao J, Lu R, Lin X, Zuo C. New threshold anonymous authentication for VANETs. IEEE/CIC International Conference on Communications in China (ICCC); 2015 Nov; IEEE, p. 1–6.
11. Azees Maria, Vijayakumar Pandi, Deboarh Lazarus J. EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks[J]. IEEE Transactions on Intelligent Transportation Systems. 2017;1–10.
12. Lu R, Lin X, Zhu H, Ho PH, Shen X. ECPP: efficient conditional privacy preservation protocol for secure vehicular communications. INFOCOM 2008. The 27th Conference on Computer Communications; 2008 Apr; IEEE; p. 1229–37.
13. Huang D, Misra S, Verma M, Xue G. PACP: an efficient pseudonymous authentication-based conditional privacy protocol for VANETs. IEEE Trans Intell Transp Syst. 2011; 12(3), 736–46.
14. Shim KA. CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks[J]. IEEE Trans Veh Technol. 2012; 61(4):1874–83.
15. Wang L, Li X, Zhong H. A revocable group batch verification scheme for VANET. SCIENTIA SINICA Informationis. 2013; 43(10), 1307–25.

16. Huang JL, Yeh LY, Chien HY. ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. IEEE Trans Veh Technol. 2011; 60(1), 248–62.
17. Bayat M, Barmshoory M, Rahimi M, Aref MR. A secure authentication scheme for VANETs with batch verification. Wireless Netw. 2015; 21(5), 1733–43.
18. Lin X, Sun X, Ho PH, Shen X. GSIS: a secure and privacy-preserving protocol for vehicular communications. IEEE Trans Vehicular Technology. 2007; 56(6), 3442–56.
19. Zong H, Huang C. Efficient group signature scheme with revocation. J. Commun. 2016; 37(10), 18–24.
20. Sucasas V, Mantas G, Saghezchi FB, Radwan A, Rodriguez J. An autonomous privacy-preserving authentication scheme for intelligent transportation systems. Comput Secur. 2016; 60, 193–205.
21. Kang J, Yu R, Huang X, Zhang Y. Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles. IEEE Trans Intell Transp Syst. 2017; 2627–2637.
22. Jiang S, Zhu X, Wang L. A conditional privacy scheme based on anonymized batch authentication in Vehicular Ad Hoc Networks[C]. IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2013 April. 7–10
23. Azees M, Vijayakumar P, Deboarh LJ. EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. IEEE Trans Intell Transp Syst. 2017; 18(9), 2467–76.
24. Next generation simulation (NGSIM) I-80 date analysis (5:00 p.m. to 5:15 p.m.) [EB/OL]. Available from: https://data.transportation.gov/Automobiles/Next-Generation-Simulation-NGSIM-Vehicle-Trajector/8ect-6jqj, 2018.
25. Hu C, Chim TW, Yiu SM, Hui LC, Li VO. Efficient HMAC-based secure communication for VANETs. Comput Netw. 2012; 56(9), 2292–303.