


RESEARCH

Open Access



A weight-based conditional privacy-preserving authentication scheme in software-defined vehicular network

Hong Zhong^{1†}, Yingxue Geng¹, Jie Cui^{1*} , Yan Xu¹ and Lu Liu²

Abstract

The rapid development of vehicular ad hoc networks (VANETs) has brought significant improvement to traffic safety and efficiency. However, owing to limitations associated with VANETs' own unchanging model and traditional network structure, there are still many challenging concerns such as poor flexibility and controllability to deal with. To solve these inherent problems effectively, we propose a weight-based conditional anonymous authentication scheme by introducing the newly emerging software-defined networking (SDN) framework. Firstly, by making use of the global planning and dynamic management features of SDN, vehicles are classified into different priorities using weighted values to reduce communications redundancy, and control the participation of malicious vehicles. Then, an efficient conditional privacy-preserving scheme was developed to secure communications among vehicles. A two-step tracing approach has been designed to exclude and punish vehicles whose weights drop below the threshold. Extensive analyses indicate that our conditional privacy-preserving scheme is secure and has lower computation costs than conventional state-of-the-art authentication schemes.

Keywords: Authentication, Software-defined vehicular network (SDVN), Weight-based system, Conditional privacy-preserving

Introduction

The application of the Internet of Things (IoT) has effectively promoted the intelligent development of all fields of life [1, 2]. These applications has made limited resources more reasonably used and distributed, thereby improved industry efficiency and effectiveness [3, 4]. Representatively, the vehicular network currently has provided people with many life-changing benefits that they may not realize. VANETs were introduced to make vehicles safer and to offer an efficient tool to enhance the driving experience. They have attracted attention from both academia and industry since inception [5]. The onboard units (OBU) installed in vehicles allow communications between vehicles (V-2-V) as well as between vehicles and

infrastructures (V-2-I) [6]. This hybrid combined network can offer many kinds of services that will bring great convenience and enhancements to current applications, such as optimum path planning, and broadcasting warnings of road accidents and other newsworthy events [7, 8]. Despite these advantages, security during communications must be considered when VANETs are used in real applications. This is for protecting the privacy of vehicles and prevent malicious users from damaging the system [9]. To overcome the shortcomings, many researchers have proposed anonymous authentication schemes to ensure secure communications [10, 11]. For instance, a conditional privacy protection authentication scheme in a multi-cloud environment [12] was proposed to secure the privacy and anonymity of vehicles by combining with cloud computing [13, 14].

However most of the present schemes are designed in traditional networks. There are some inherent problems

*Correspondence: cuijie@mail.ustc.edu.cn

[†]Hong Zhong contributed equally to this work.

¹School of Computer Science and Technology, Anhui University, Jiulong Road, 230039 Hefei, China

Full list of author information is available at the end of the article

in traditional networks, such as they can not suit the fastly changing topology of VANETs and may cause some uncontrollable security threats. Chen et al. [15] gave a survey on security problems on Software Defined Mobile Network (SDMN). To some extent, SDVN is similar to SDMN, such as the fast changing topology, as well as frequent joining and leaving. By this we got inspired to introduce SDN into VANETs to cope with those security problems. The survey of Jaballah et al. [16] gave a new direction to resolving the privacy problem in VANETs by including SDN technology [17].

SDN is a newly emerging and promising technology that breaks the traditional network model by decoupling the control and data planes. In the control plane, all the managing and monitoring functions are logically united into one entity called a controller. The data plane includes all kinds of wired or wireless networking infrastructure used to forward network traffic. In this way, the system can release routing-related equipment from heavy forwarding jobs using the programmable properties of SDN to ease and enhance the overall network performance [10].

This new network architecture has received significant attention from mobile networks such as VANETs for its abilities to enhance performance, flexibility, and scalability [18]. By concentrating all protocol-specific features in the software, this extension of the SDN paradigm is expected to incorporate mobile network specific functionality [19]. Moreover, the new architecture also brings new opportunities and approaches to cope with some inherent problems in traditional networks, especially regarding security [20]. There have been some studies dedicated to solving security problems in the control plane [21], such as distributed denial-of-service and malware attacks. However, the security and privacy problems existing in the data plane have not received focus.

We are proposing a conditional privacy-preserving scheme, which is used to protect the communication security and improve network efficiency in a SDVN framework. In our scheme, a weigh-based is offered to execute the first-step detection as a filter to lower the message density. As background, the detailed work process and weighting system will be explained in “Background” section.

Our contributions

In this paper, we propose a conditional authentication scheme that offers a weight-based system to monitor malicious vehicles when protecting the privacy of vehicles in SDVNs. The main contributions of our scheme are threefold.

- 1 To support communication privacy and efficient traceability in SDVNs, a message privacy-preserving authentication scheme is proposed with two-step

tracing. The authentication scheme relieves local controllers of the need to store information about vehicles and system parameters. The layered controller model also relieves the global controller of the heavy work burden of computation and reduces deployment costs.

- 2 We have built a framework of weight-based incentive system by offering vehicles candidate forwarding sets (CFSS) in the SDVN framework to encourage vehicles to upload correct and real-time information about traffic and roads. Information uploaded by vehicles will be used to enhance driving experiences like route planning and avoiding traffic congestion. This system evaluates vehicles and sets their priorities according to their weight values. Vehicles with low weight values will lose trust from controllers after a specific period.
- 3 Extensive analyses are performed to prove the security and efficiency of the proposed scheme.

Organization of this paper

The remainder of this paper is organized as follows. “Related work” section introduces the related works. “Background” section tells the system model and some background acknowledges used in our study. “Proposed scheme” section presents our specific scheme. Then, “Security proof and analysis” section shows the detailed security proof and analysis. In “Performance analysis” section, we give the performance evaluation and comparison. Finally, “Conclusion” section gives the conclusion and some concluding remarks.

Related work

There have been many works dedicated to designing efficient conditional privacy-preserving schemes [13, 22–25] to secure vehicles’ identities and communications [26–28]. With the advent of SDN technology, some research areas including VANETs have realized the convenience and advantages of this new network architecture. SDN has been introduced to address some inherent problems in [10, 13, 21, 29–33].

Shao et al. [34] proposed an anonymous authentication protocol for VANETs by using a new group signature scheme, which achieved threshold authentication and group signature in VANETs. However, massive and heavy computation overhead coming with bilinear pairing operation and map-to-point hash operation may strictly limit its practicability.

Lai et al. [35] proposed an integrated network architecture for secure group communication in SDN-based 5G-VANETs. With this scheme, some security challenges in both decentralized and centralized networks can be addressed and the performance evaluation proved to be outstanding, but it lacks a detailed concrete privacy-

preserving approach to guarantee vehicles' privacy. In [36], they introduced a unified secure and seamless IP communications framework for a group-oriented heterogeneous vehicular environment. The framework aimed to make use of the advantages of a SDN structure to set up the platoon securely and flexibly and control the handover signaling overload.

Cui et al. [37] designed an authentication protocol for 5G-enabled vehicular networks in which TA is in charge of the reputation management to filter vehicles with a reputation score below a given threshold, which reduces the existence of untrusted messages in VANETs. Zhang et al. [38] proposed a novel Chinese remainder theorem based conditional privacy-preserving authentication scheme to secure vehicular authentication. This scheme solved the leakage problem during side channel attacks and ensured security for the entire system.

Jaballah et al. [16] gave a detailed survey on SDVNs that introduced benefits, future directions and existing challenges, especially about communications security.

Garg et al. [39] presented a SDN based privacy-preserving scheme for vehicular networks at a 5G perspective. The scheme provided end-to-end security methods through its inbuilt modules including authentication and intrusion detection. The authentication scheme relies on ECC to authenticate the CA, CH, and the vehicles before data transmission. And the intrusion detection employs the concept of tensor-based dimensionality reduction to reduce the size of vehicular traffic data then expose it for detection. However, this scheme only introduced the identity authentications between CA and CH as well as CH and vehicles. The further message authentication scheme was not designed to secure communication. In addition, the authentication scheme may require too much computation and storage which will cause great overhead and delay while deploying.

Huang et al. [40] proposed 5G software-defined vehicular network model. Based on that, a conditional privacy-preserving authentication scheme which avoided single point of failure problems and using of ideal tamper-proofed device and certificate revocation list (CRL). The scheme used a revocation list to reduce the verification delay caused by checking the long CRL, and storage coming with the large number of pseudonyms in the CRL. However, every second pseudo identity (SPID) of V_i has a validation time and can only be used once, then it will be removed from the list. This design will cost too much storage and computation overhead while tracking the real identities of malicious vehicles.

Background

In this section, we formalize the weight value computation system. Assumptions and security goals will be elaborated in detail as well.

System model

The proposed system model is composed of the following entities: global controller (*GC*), local controller (*LC*), the deployed access point (*AP*) and cellular network base station (*BS*), transport manager (*TM*) and *OBUs* that are preloaded on the vehicles, as presented in Fig. 1. Functions of these network entities and related assumptions will be demonstrated followed.

- 1 *GC*: The global controller of this system has extremely outstanding computing and storage capabilities compared with *LCs* and *OBUs*. In the narrower SDN system, the controller is a logic centralized strategy point based on OpenFlow protocol, and responsible for managing traffic flow, route discovery, and other control work. In our scheme, like the traditional Trusted Authority, the *GC* takes responsible for some heavy computation missions like generating and distributing system parameters, as well as updating them periodically. Beyond that, the *GC* also monitors and manages the global network, including updating route strategy and detecting malicious members. When necessary, the *GC* will take part in tracking real identities of vehicles.
- 2 *LC*: Local controllers in the scheme are designed mainly for balancing the computation burden of the *GC*, and decline the cost of deployment considering the real situation. The layered structure is shown in Fig. 2. Each local controller takes charge of one specific area. Like the traditional Roadside Units, when received the requesting message including the real identity from a vehicle, the *LC* will return the pseudo-identity, the secret key, and some other parameters to the sender. Beyond that, *LCs* also make local route strategy, compute weight values, and execute some other controlling actions. But in consideration of security and storage costs, *LCs* will not store any of these identities entries. When there is a necessity to track the true identity, the *LC* will check if it has the ability to extract. If not, it submits the message to *GC*. Tracking steps will be presented in "Proposed scheme" section in detail.
- 3 *OBU*: *OBU* is a computing unit that is preloaded in the vehicle. *OBUs* get access to wireless networks and offer vehicles various network services like navigation and disaster warning. Besides, *OBUs* submit vehicle conditions and surrounding traffic situations. These feedback will be used by *LCs* and *GC* to get overall planning for vehicles themselves [41].
- 4 *AP* and *BS*: Vehicles in our system can get access to not only cellular networks like 3G/4G/5G, but also city WiFi via access points and other types of networks. For ubiquitous 5G base stations still

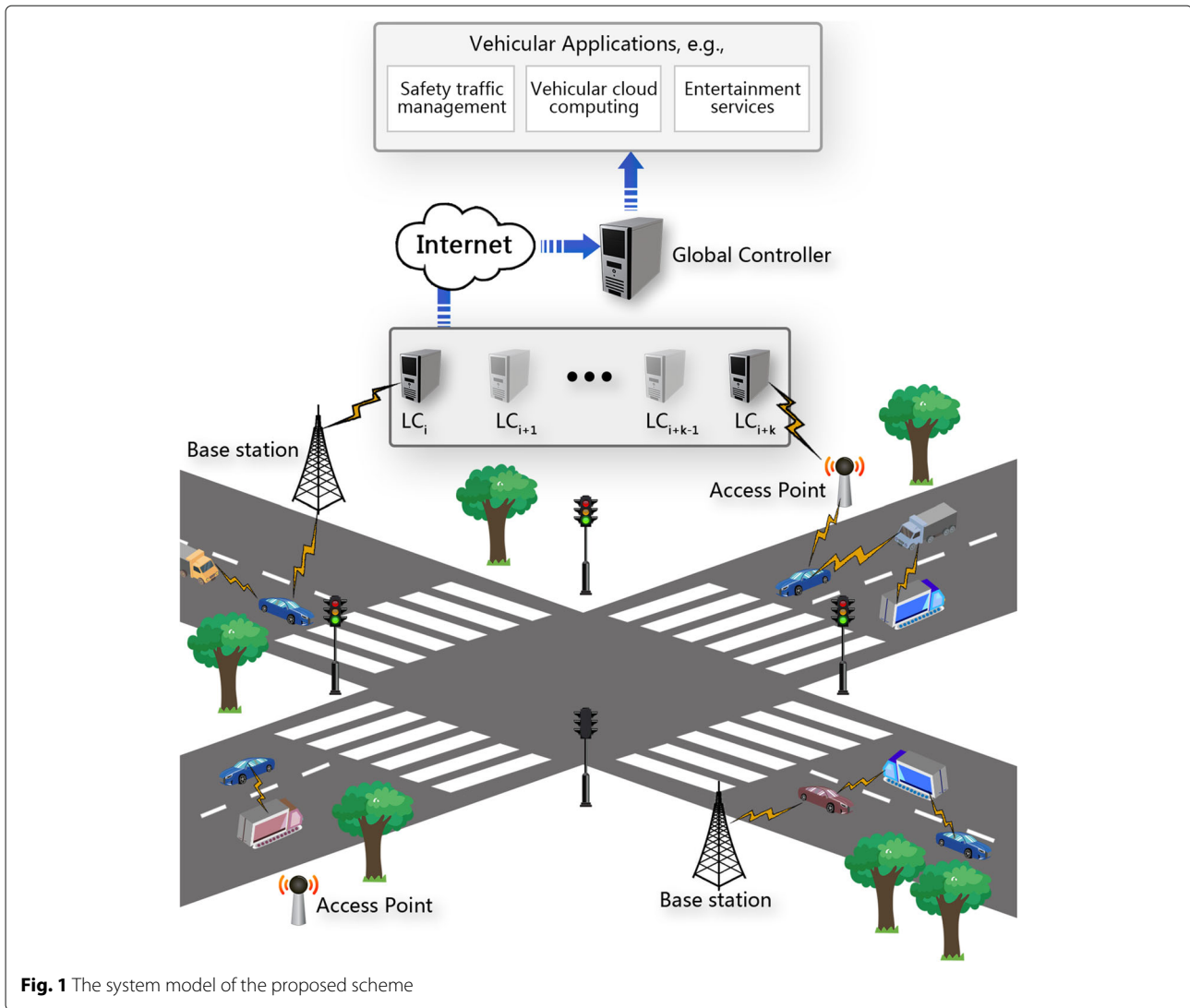


Fig. 1 The system model of the proposed scheme

requires a quite long period to deploy, and the cost may be unaffordable for some users. So the coexistence of different types of networks is necessary.

- 5 *TM*: Transport manager is the vehicle-managing authority. It would notify and warn vehicle owners when their vehicles' weight values drop below a specific threshold value.

The system assumptions are presented as below:

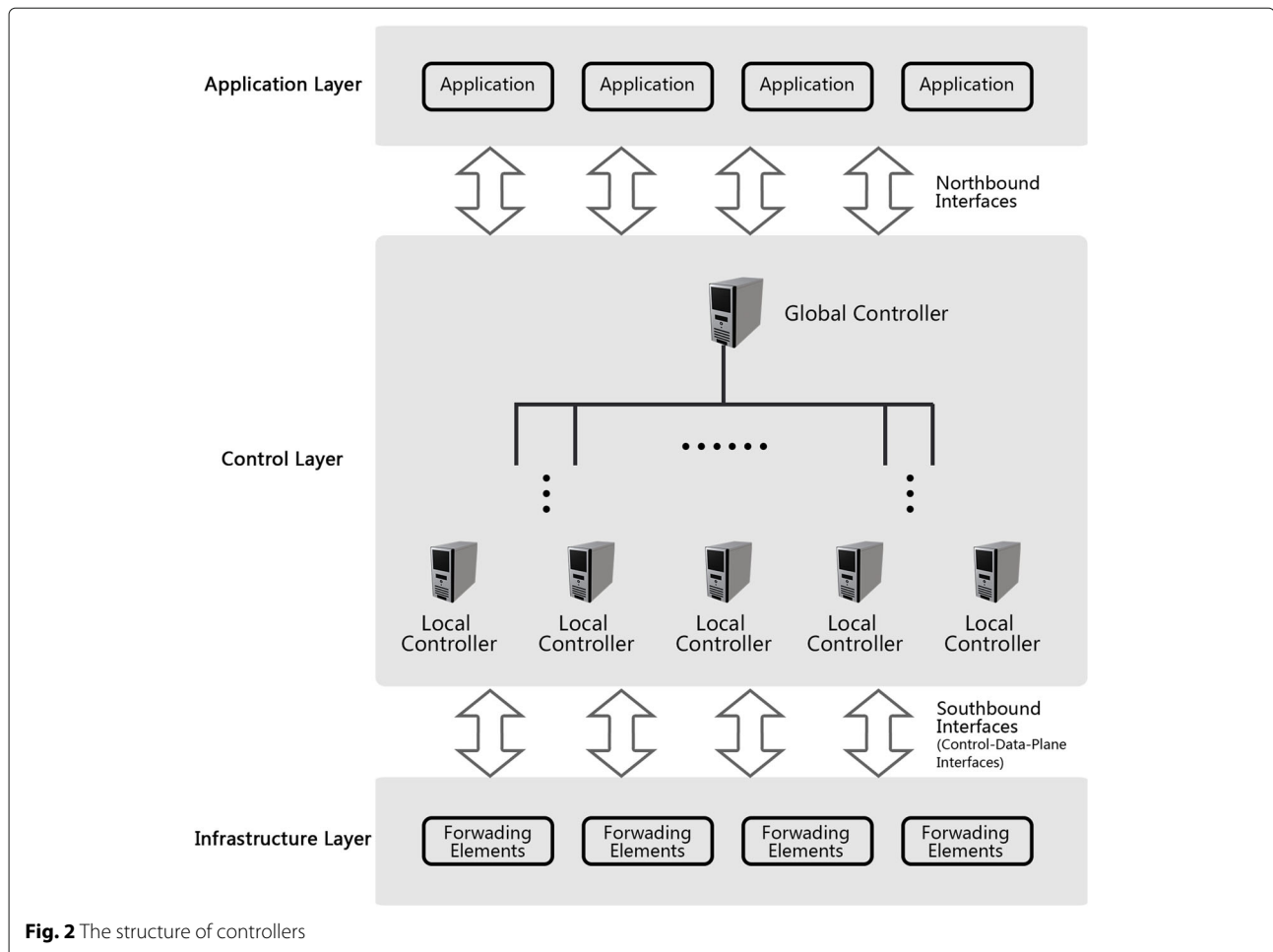
- The *GC* is completely trustable and can not be compromised.
- *LCs* is trusted but their capabilities are limited and far from taking place of the *GC*.
- Vehicles are half-trusted, but the vital parameters stored inside are not available to adversaries.
- The overall roads map and building distribution have been preloaded in *GC*. Local maps and distributions are preloaded in corresponding *LCs*.

Controllers in our scheme are only responsible for traffic managing and route planning or other network-related affairs. Vehicles management and other social service applications will be allowed to plug into the unified north APIs offered by controllers.

Weight computation system

In our proposed model, the weight computation system computes *CFSs* for vehicles. According to vehicles' weight values in the current period, the system will classify them into different priorities for vehicles in the present area [37]. By introducing this model, vehicles that have sent too many bogus messages will be squeezed out of the high priority set. More invalid or fake messages they send, lower priorities will be labeled on them. The main mechanism of this part is shown in Fig. 3.

- 1 When the vehicle V_i intends to send messages in the current area, it will request present parameters and its *CFS* via wireless network.



2 When received requested messages from vehicles, the LC will return security parameters and corresponding CFSs according to preloaded road maps and conditions of vehicles. The main elements that should be considered in our environment are:

- (a) Relative Distance (*RD_{st}*): Denotes the relative distance between V_i and other vehicles according to their relative speeds.
- (b) Remaining Power (*P_{wr}*): Denotes the remain power including computing and storing capabilities of vehicles in the current areas. Vehicles with low remaining power may will not be able to afford other missions while satisfying their own needs.
- (c) Network Situation (*NS*): Denotes the network situations that vehicles getting access to including average expenses and traffic speeds.
- (d) Bogus Message (*BM*): Denotes the number of messages that a vehicle has sent in one specific period. In one accumulation cycle, the first time it gets detected, its *BM* value will be set as s . The second time, $s = s + n1s$, $n1$ is an

appropriate coefficient that suits the present environment of this area. Similarly, the third bogus message will make $s = n + n1s + n2s$, $n1 \geq 1$, $n2 \geq 1$, and so on. It means that more bogus messages are detected from one vehicle, its weight value drops more quickly than constant multiple speed.

- (e) Other Elements (*OE*): There are a lot of roads conditions that should be taken seriously such as the distributions of buildings. For example, since the deployment of new 5G base stations are under way, the feature that its signal suffers more serious loss compared with other cellular networks should be taken into consideration. And if vehicles tend to transmit files like streaming files, the size of messages and their priorities must be taken into consideration as well, for there are great differences among the expenses of different networks.

Take all the elements into count, the final weight computation formula would be

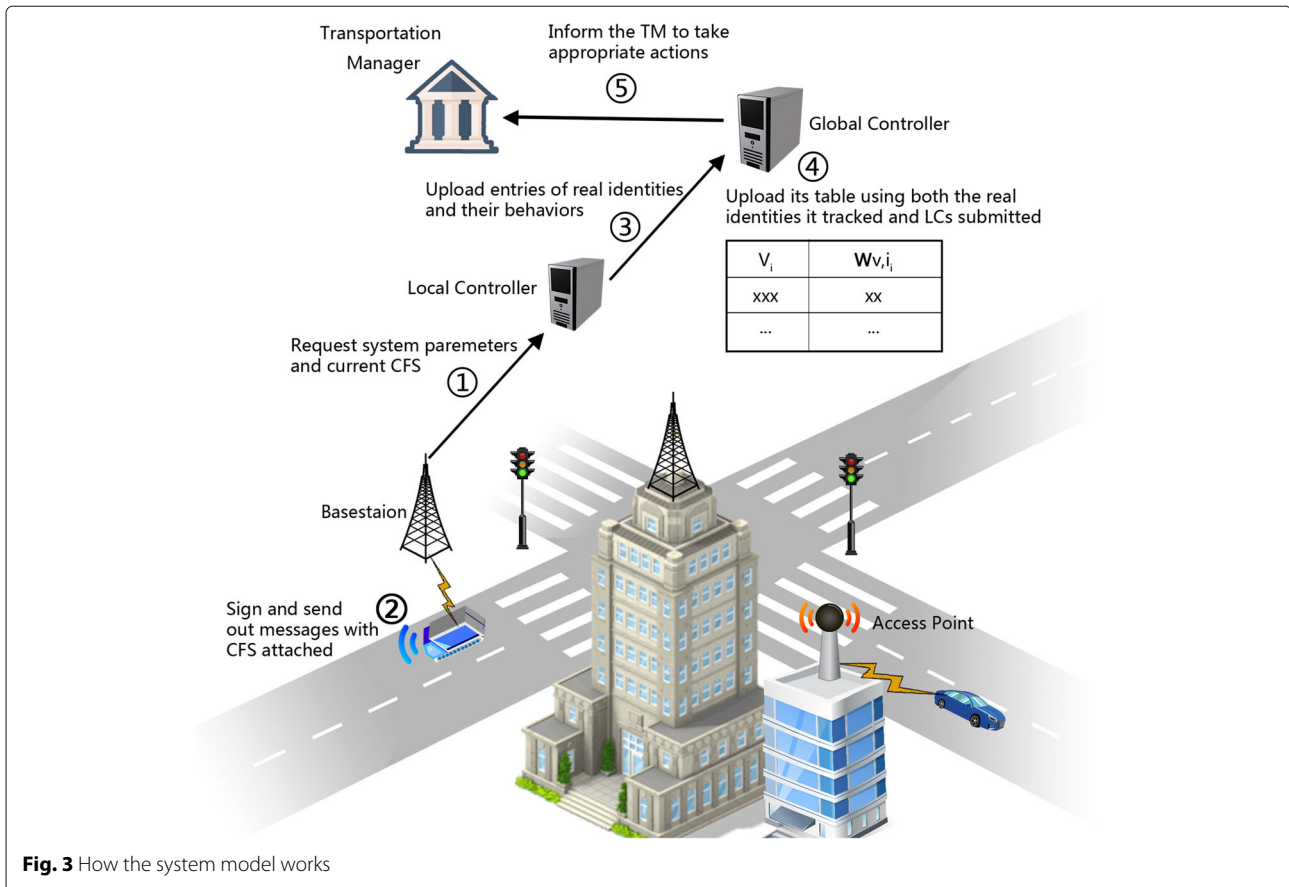


Fig. 3 How the system model works

$$W_{v,i} = w_1RDst + w_2Pwr + w_3NS + w_4BM + w_5OE. \tag{1}$$

where $w_1 + w_2 + w_3 + w_4 + w_5 = 1$. After computing all the weight values in the area, the LC will set their priorities. Here we set priorities as four levels: L1 (prior), L2 (sub-prior), L3 (medium) and L4 (low). The priorities calculation method is shown as Algorithm 1. Then the LC returns security parameters with the CFS to the requesting vehicle. When all necessary contents are acquired, the vehicle will sign messages via the authentication scheme demonstrated in the next section. Then it sends out messages with the CFS attached as Algorithm 2 shows. If received messages, vehicles will check its priority in the CFS. If its priority is L1, it forwards without waiting. If the priority level is lower than L1, it awaits for a specific period. If vehicles do not receive ACK packages from the higher-level ones in this period, they forward [29]. Since the CFS is not integrated with any specific routing algorithm, it can be applied with all kinds of routing models to offers better candidates.

3 When an accumulation phase ends, LCs will upload to the GC entries of vehicles' information. The

numbers of bogus messages vehicles had sent in the previous period will be recorded.

- 4 Received real-time entries from LCs, the GC will upload its table with both the real identities it tracked and LCs submitted.
- 5 When vehicles are found their weight values have dropped below the threshold value, the GC will inform TM to take appropriate actions.

Security goals

Here we introduce the main security goals that our proposed scheme is aimed to achieve.

- 1 *Authentication*: Messages issued by vehicles should be signed by senders so that receivers could verify the integrity and authenticity of messages.
- 2 *Identity Privacy Preserving*: Vehicles in our model use pseudo identities to communicate, so that no third party with no authorization could track vehicles' real identities.
- 3 *Traceability*: Though vehicles use pseudo identities to communicate, controllers need to be able to track their real identities when it's necessary.
- 4 *Unlinkability*: Adversaries are not able to link messages sent by the same vehicle or to trace the vehicle's movement tracks.

Algorithm 1 Program to decide V_i 's priority

Data: $W_{v,i}, L^*_{limit}$
 // $W_{v,i}$ represents the weight value of V_i , L^*_{limit} denotes the lower limit of priority L^*
Result: The priority of V_i based on $W_{v,i}$

- 1: **begin**
- 2: **if** $W_{v,i} \geq L1_{limit}$ **then**
- 3: V_i is appended to Set_{L1} // Set_{L1} denotes the set of priority of $L1$
- 4: **else if** $W_{v,i} \geq L2_{limit}$ **then**
- 5: V_i is appended to Set_{L2} // Set_{L2} denotes the set of priority of $L2$
- 6: **else if** $W_{v,i} \geq L3_{limit}$ **then**
- 7: V_i is appended to Set_{L3} // Set_{L3} denotes the set of priority of $L3$
- 8: **else**
- 9: V_i is appended to Set_{L4} // Set_{L4} denotes the set of priority of $L4$
- 10: **end if**
- 11: **end**

5 *Resistance to Attacks:* The proposed scheme is able to resist various other common attacks, for example, forgery attack, replay attack, impersonation attack, modification attack, and man-in-middle attack.

Algorithm 2 Process to issue messages in our scheme

Data: ID_i, M
 // ID_i denotes the real identity of V_i , M represents the message to be sent
Result: Signed message with CFS attached

- 1: **begin**
- 2: **Step 1:** Registration
- 3: V_i sends its identity ID_i to LC
- 4: **Step 2:** Assessment
- 5: **if** $W_{v,i} < Threshold$ **then**
- 6: LC refuses the request
- 7: **else**
- 8: LC evaluates the environment of V_i
- 9: Computes CFS
- 10: Computes $PID_{v,i} \leftarrow PseudoIDFunction(ID_i)$,
 $SK_i \leftarrow SecretKeyFunction(PID_{v,i})$
- 11: // $PID_{v,i}$ denotes the pseudo identity of V_i , SK_i denotes the communication secret key of V_i
- 12: **end if**
- 13: **Step 3:** Signature
- 14: V_i signs M and issues out with CFS attached
- 15: **end**

Proposed scheme

To achieve privacy-preserving and efficient traceability while communicating, the authentication scheme designed for our SDVN environment will be presented in detail in this section. Firstly, the GC chooses parameters and distributes them. When a LC receives parameters, it will set the system. Then if a vehicle enters into the managing range of the LC and requires to sign and send messages, the LC will choose the best CFS and send to it. Then the vehicle broadcasts the signed message with the CFS attached. Adjacent vehicles will check if they are in the CFS . If in, it verifies the message and decides to abandon or transfer. If it is necessary to track the identities of vehicles, our scheme offers a two-step tracing approach, which balances the computations and storage overloads of LCs and the GC to the greatest extent.

System initialization

Let F_p be a finite field, and p be a large prime number and the size of the field. $(a, b) \in F_p$ are the parameters of the elliptic curve of E . P is the generator and q is the prime order of E . Some notations and definitions in our scheme are presented in Table 1.

- 1 The GC chooses $H0 : \{0, 1\}^* \rightarrow Z_q^*$,
 $H1 : \{0, 1\}^* \times G \rightarrow Z_q^*$, $H2 : \{0, 1\}^* \times G \rightarrow Z_q^*$,
 $H3 : \{0, 1\}^* \rightarrow Z_q^*$,

Table 1 Notations and definitions

Notations	Definitions
GC	The Global Controller
LC_i	Local Controller i
V_j	The j -th vehicle
G	An elliptic curve cycle additive group
P	A generator of G
q	The order of G
p	The size of a field
F_p	A finite field
Z_q^*	The residue system modulo prime q
ID_j	The identity of V_j
$PID_{v,j}$	The pseudo identity of V_j
P_{pub}	A public key of controllers
s	A private key of controllers
SK_j	A private key of V_j
M	A message
msg	A encapsulated message
σ	The signature of a message
T_t	The time stamp
\parallel	The message concatenation operation
\oplus	The exclusive-OR operation

$H4 : \{0, 1\}^* \times \{0, 1\}^* \times G \times \{0, 1\}^* \times \{0, 1\}^* \rightarrow Z_q^*$. Then it randomly selects $\alpha, \beta, s \in Z_q^*$, s as the secret key and $P_{pub} = sP$ as the public key of controllers system. Then the GC transmits parameters to LC_i via secure channels.

- 2 When the LC_i receives parameters generated by GC , it computes $A = \alpha \cdot P \cdot H0 (PID_{LC,i})$, $B = \beta \cdot P$, where $PID_{LC,i} = ID_i \oplus H1 (P_{pub} \| B)$. Then LC_i publishes $\{H0, H1, H2, H3, H4, P, P_{pub}, q, PID_{LC,i}, A, B\}$ as the present system parameters.
- 3 To successfully track the identities of vehicles when necessary, the GC stores a 5-tuple $(PID_{LC,i}, P_{pub}, T_{start}, T_{end})$. T_{start} and T_{end} means the enabling and disabling times respectively of secret keys s . To save computation cost, secret keys can serve irregular circularly. But to ensure the security of controllers, LC_i don't save any of them.

Vehicles registration

When vehicle V_j enters into the range of the LC_i , it sends request message including its identity $ID_{v,j}$ to the LC_i . Then LC_i computes $PID_{v,j} = LC_i \oplus H2 (s \| B)$ as its pseudo identity, $SK_j = \alpha \cdot H3 (PID_{v,j})$ as its secret key.

Message signing and verifying

When V_j tends to communicate with other entities, it signs and encapsulates messages with attached data such as CFS_j . Surrounding vehicles will check if they are in CFS_j . If not, they retain the message for temporary and wait for ACK packages. Else they verify the signature then reforward it with its own CFS .

- 1 V_j randomly chooses a number $r_j \in Z_q^*$ and lets $R_j = r_j \cdot P$. And V_j signs message M with computing

$$\sigma = SK_j \cdot H0 (PID_{LC,i}) + r \cdot H4 (M \| PID_{LC,i} \| R_j \| T_t \| CFS_j) \text{ mod } q \quad (2)$$

where M denotes related message and T_t is the timestamp.

- 2 Then V_j issues out the message msg as the form of $\{M \| R_j \| PID_{v,j} \| PID_{LC,i} \| T_t \| \sigma \| P_{pub} \| CFS_j\}$.
- 3 To verify the message received, firstly timestamp T_t is checked. If it's still fresh, then (3) will be verified if it holds.

$$\sigma \cdot P = A \cdot H0 (PID_{v,j}) + r \cdot H4 (M \| PID_{LC,i} \| R_j \| T_t \| CFS_j) \text{ mod } q. \quad (3)$$

Batch Verification: When a vehicle receives n messages in a short interval, verifying them piece by one will consume lots of time and energy. So our scheme allows batch verification. Firstly, receiver checks if $T_{t,1}, T_{t,2}, \dots, T_{t,n}$ are fresh. Then it selects n

ephemeral values e_1, e_2, \dots, e_n randomly, where $e \in [1, 2^t]$ and t is a small integer. Finally, receiver verifies whether Eq. (4) holds.

$$\sum_{j=1}^n (e_j \cdot \sigma_{v,j}) \cdot P = \left(\sum_{j=1}^n e_j \cdot A_j \cdot H0 (PID_{v,j}) \right) + \left(\sum_{j=1}^n e_j \cdot R_j \cdot H4 (M \| PID_{LC,i} \| R_j \| T_t \| CFS_j) \right). \quad (4)$$

Identity tracking

As we mentioned before, our scheme provides a two-step tracking approach to track a vehicle's real identity when it is found the weight value drops below a certain threshold.

- 1 LC extracts P_{pub} from msg and judges if it equals the present P_{pub} . If it's the present used parameter, the LC computes $ID_{v,j} = PID_{v,j} \oplus H2 (s \| B)$. If P_{pub} extracted from msg does not equal to the serving one, it means the parameter expired or not published by the present LC , then the LC retransmits the message to GC .
- 2 GC extracts P_{pub} and T_t from msg . With T_t it can rapidly locate the corresponding tuple and find out the old secret key s in its storage. Then it computes and gains the real identity $ID_{v,j} = PID_{v,j} \oplus H2 (s \| B)$. And based on protocols and laws, GC will blacklist vehicles for a certain period or refuse to offer services. Moreover, GC can submit malicious user's list to related arbitration or credit managing apartment like TM .

Security proof and analysis

Security proof

Firstly the definition of the elliptic curve discrete logarithm problem (ECDLP) that the whole analysis based on will be introduced.

Definition1 (ECDLP): $n \in Z_q$ and $N = nP \in G$, where P is the generator of the group G . Given $N = nP$ it's difficult to compute n . Then a game between adversary \mathcal{A} and challenger \mathcal{C} is introduced to set up the security model of our scheme.

Setup Oracle: In this query, \mathcal{C} generates the secret keys and other system parameters, which are sent to \mathcal{A} .

H0 Oracle: On input m by \mathcal{A} , \mathcal{C} chooses a random number r from Z_q and returns to \mathcal{A} while inserting the tuple (m, r) into list L_{H0} .

H1 Oracle: On input m by \mathcal{A} , \mathcal{C} chooses a random number r from Z_q and returns to \mathcal{A} while inserting the tuple (m, r) into list L_{H1} .

H2 Oracle: On input m by \mathcal{A} , \mathcal{C} chooses a random number r from Z_q and returns to \mathcal{A} while inserting the tuple (m, r) into list L_{H2} .

H3 Oracle: On input m by \mathcal{A} , \mathcal{C} chooses a random number r from Z_q and returns to \mathcal{A} while inserting the tuple (m, r) into list L_{H3} .

H4 Oracle: On input m by \mathcal{A} , \mathcal{C} chooses a random number r from Z_q and returns to \mathcal{A} while inserting the tuple (m, r) into list L_{H4} .

Sign Oracle: In this query, on receiving message M from \mathcal{A} , \mathcal{C} generates msg and sends to \mathcal{A} .

If adversary \mathcal{A} could generate a login request message, it is proved to be able to violate the authentication of the scheme. Let $\Phi(\mathcal{A})$ denote the probability that \mathcal{A} violates the authentication of our scheme.

Definition 1. Our scheme is secure if $\Phi(\mathcal{A})$ is negligible for any polynomial adversary \mathcal{A} .

We evaluated the proposed scheme and it is proved secure in the random oracle.

Theorem 1. The proposed scheme is secure in the random oracle model.

Proof: Suppose that there exists adversary \mathcal{A} that could forge a msg . We construct a challenger \mathcal{C} that is able to solve the ECDLP problem with a non-negligible probability by running \mathcal{A} as a subroutine.

Setup Oracle: Firstly a security parameter k is taken as input. Then \mathcal{C} randomly selects a number s as its private key and computes $P_{pub} = sP$ and \mathcal{C} sends $\{H0, H1, H2, H3, H4, P, P_{pub}, q, PID_{LC,i}, A, B\}$.

H0 Oracle: \mathcal{C} keeps a list $L_{H0}(PID_{LC,i}, h0)$ initialized to empty. When \mathcal{A} invokes this query with $\langle PID_{LC,i} \rangle$, \mathcal{C} checks if $\langle PID_{LC,i}, h0 \rangle$ already exists in L_{H0} . If so, \mathcal{C} returns $h0$. Otherwise it generates a random $h0 = H0(PID_{LC,i})$, inserts $\langle PID_{LC,i}, h0 \rangle$ in L_{H0} and returns $h0$ to \mathcal{A} .

H1 Oracle: \mathcal{C} keeps a list $L_{H1}(P_{pub}, B, h1)$ initialized to empty. When \mathcal{A} invokes this query with $\langle PID_{LC,i}, B \rangle$, \mathcal{C} checks if $\langle P_{pub}, B \rangle$ already exists in L_{H1} . If so, \mathcal{C} returns $h1$. Otherwise it generates a random $h1 = H1(P_{pub}||B)$, inserts $\langle P_{pub}, B, h1 \rangle$ in L_{H1} and returns $h1$ to \mathcal{A} .

H2 Oracle: \mathcal{C} keeps a list $L_{H2}(s, B, h2)$ initialized to empty. When \mathcal{A} invokes this query with $\langle s, B \rangle$, \mathcal{C} checks if $\langle s, B \rangle$ already exists in L_{H2} . If so, \mathcal{C} returns $h2$. Otherwise it generates a random $h2 = H2(s||B)$, inserts $\langle s, B, h2 \rangle$ in L_{H2} and returns $h2$ to \mathcal{A} .

H3 Oracle: \mathcal{C} keeps a list $L_{H3}(PID_{v,j}, h3)$ initialized to empty. When \mathcal{A} invokes this query with $\langle PID_{v,j} \rangle$, \mathcal{C} checks if $\langle PID_{v,j} \rangle$ already exists in L_{H3} . If so, \mathcal{C} returns $h3$. Otherwise it generates a random $h3 = H3(PID_{v,j})$, inserts $\langle PID_{v,j}, h3 \rangle$ in L_{H3} and returns $h3$ to \mathcal{A} .

H4 Oracle: \mathcal{C} keeps a list $L_{H4}(M, PID_{v,j}, T_t, R_j, CFS_j, h4)$ initialized to empty. When \mathcal{A} invokes this query with $\langle M, PID_{v,j}, T_t, R_j, CFS_j \rangle$, \mathcal{C} checks if $\langle M, PID_{v,j}, T_t, R_j, CFS_j \rangle$ already exists in L_{H4} . If so, \mathcal{C} returns $h4$. Otherwise it

Table 2 Running time of operations

Operations	Running Time(ms)
T_m	0.3218
T_a	0.0024
T_h	0.001

generates a random $h4 = H4(M||PID_{v,j}||T_t||R_j||CFS_j)$, inserts $\langle M, PID_{v,j}, T_t, R_j, CFS_j, h4 \rangle$ in L_{H4} and returns $h4$ to \mathcal{A} .

Sign Oracle: On receiving \mathcal{A} 's query with message M and pseudo identity $PID_{v,j}$, \mathcal{C} chooses random α, β, R_j from Z_q and computes signature $\sigma = \alpha H0(PID_{LC,i}) + H4(M||PID_{LC,i}||R_j||T_t||CFS_j)$. Then \mathcal{C} inserts $\langle PID_{LC,i}, h0 \rangle$ and $\langle M, PID_{v,j}, T_t, R_j, CFS_j, h4 \rangle$ into L_{H0} and L_{H4} respectively.

Analysis: Based on Forking lemma [42], suppose that \mathcal{A} has generated two valid signatures $\sigma = SK_j H0(\cdot) + r H4(\cdot)$ and $\tilde{\sigma} = SK_j \tilde{H0}(\cdot) + \tilde{r} \tilde{H4}(\cdot)$. To obtain the secret key SK_j , it computes

$$\frac{\sigma - \tilde{\sigma} - r \cdot H4(\cdot) + \tilde{r} \cdot \tilde{H4}(\cdot)}{H0(\cdot) - \tilde{H0}(\cdot)} \bmod q = SK_j \quad (5)$$

As the result shows, \mathcal{C} is able to solve the ECDLP problem as a polynomial adversary, which contradicts Definition 1. So we come to the conclusion that the proposed scheme is secure against adaptive chosen message attack in the random oracle model.

Security and attributes analysis

- Authentication:** According to Theorem 1, there exists no polynomial adversary being able to forge a valid message. Therefore the integrity of messages are able to be verified by computing $\sigma \cdot P = A \cdot H0(PID_{v,j}) + r \cdot H4(M||PID_{LC,i}||R_j||T_t||CFS_j) \bmod q$.
- Identity Privacy Preserving:** The vehicle's real identity does take part in the communication process but in the form of pseudo identity, and the master key stays unexposed. If an adversary intends to obtain other vehicle's identities, it has to solve the difficult problems in mathematics in our scheme, which makes sure the identity privacy preserved.
- Traceability:** If messages are found dishonest while transporting, LC s or GC can obtain the identities of vehicles by computing $ID_{v,j} = PID_{v,j} \oplus H2(s||B)$.
- Unlinkability:** As a result of using different pseudo identities in different areas or even different periods, adversaries are kept from figuring out if multiple messages come from one same vehicle.
- Resistance to Attacks:** The proposed scheme can also resistant the following attacks [43, 44].

Table 3 Comparisons of computational overhead

Scheme	Signature	Single Authentication	Batch Authentication
He et al. [11]	$3T_m + 3T_h$	$3T_m + 2T_a + T_h$	$(n + 2)T_m + (3n - 1)T_a + 2nT_h$
Li et al. [24] (EPA-CPPA)	$1T_m + 2T_h$	$4T_m + 1T_a + 2T_h$	$(2n + 2)T_m + (n)T_a + (2n)T_h$
Li et al. [45]	$1T_m + 1T_h$	$3T_m + 3T_a + 2T_h$	$(n + 2)T_m + (3n)T_a + (2n)T_h$
Our scheme	$1T_m + 2T_h$	$T_m + T_a + 2T_h$	$(n)T_m + (n)T_a + (2n)T_h$

- **Forgery Attack:** This attack intends to forge and transmit false warning messages in order to contaminate roads information and mislead vehicles. In the proposed scheme, once a vehicle found to send out false messages, its weigh value will drop more quickly than constant multiple speed. At last, the messages transformed by this vehicle will be ignored by surrounding vehicles.
- **Replay Attack:** The encapsulated message contains timestamps, which can prevent messages are saved then reforwarded. Receivers check the freshness of messages at the very first beginning when getting them.
- **Impersonation Attack:** If an adversary tends to impersonate a legal vehicle, it must generate a signature of the related message which satisfying $\sigma \cdot P = A \cdot H_0(PID_{v,j}) + r \cdot H_4(M \parallel PID_{LC,i} \parallel R_j \parallel T_t \parallel CFS_j)$, which is difficult according to Theorem 1.
- **Modify Attack:** If the message contained is modified, receivers will find out that the equation doesn't hold. Then modified illegal message will be abandoned.
- **Man – in – the – middle Attack:** Since messages sent by senders and receivers needs to be verified its integrity and non-reputation, the scheme can resist man-in-the-middle attack.

Performance analysis

In this section, we are going to analyse the performance of our scheme with comparison of schemes of He et al. [11], Li et al. [24] (EPA-CPPA) and Li et al. [45]. First, we set the order q of group G on the super elliptic curve $E : y^2 = x^3 + ax + b \text{ mod } p$, ($a, b \in Z_p^*$), in which q, p are 160-bit prime numbers. The notations used in this part are presented as below:

- 1 T_m : The time spent on performing a scale multiplication operation $x \cdot P$, where $x \in Z_p^*, P \in G$.
- 2 T_a : The time spent on performing a point addition operation $Q + R$, where $Q, R \in G$.
- 3 T_h : The time required for performing an one-way hash function operation.

To compare fairly, we implemented the cryptographic operations in the following environment. The processor is Intel Core CPU i7-6700 at 3.40 GHz and 8 GB RAM, and the operating system is Windows 7. Table 2 gives running times of performing those operations. The analysis is parted into three aspects: signing a single message, single message verification, and batch messages verification. In the scheme of He et al. [11], to sign a single message, three scale multiplications and three one-way hash functions are required, which is $3T_m + 3T_h \approx 0.9684 \text{ ms}$. When to verify a single message, it costs three scale multiplications, two point additions and two one-way hash

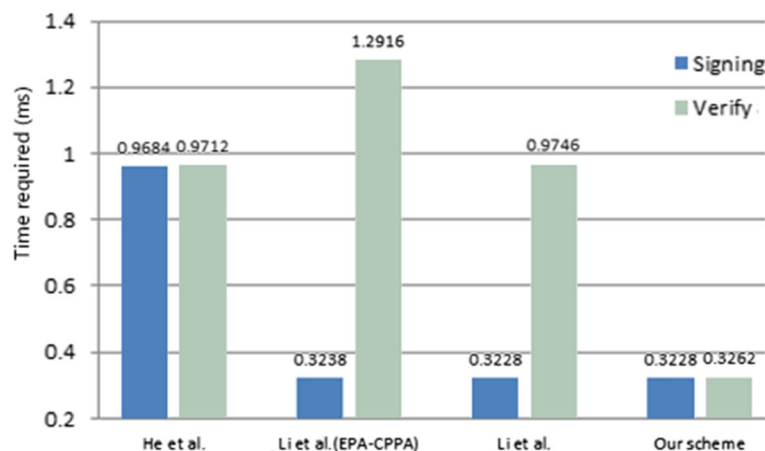


Fig. 4 Computation overhead of signing and verifying

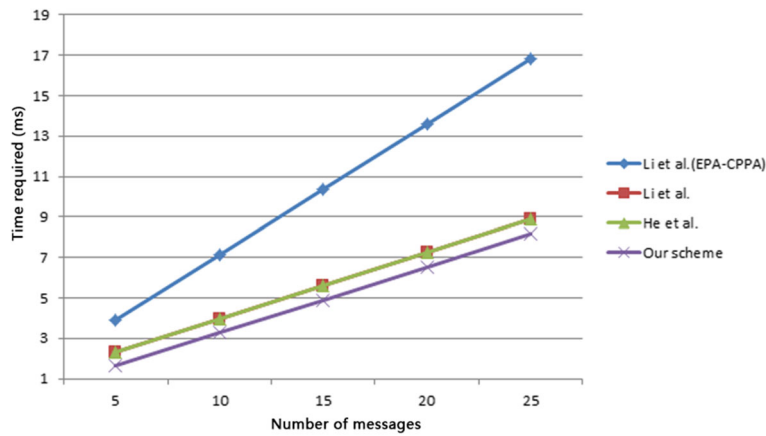


Fig. 5 Computation overhead of batch verifications

functions, which is $3T_m + 2T_a + T_h \approx 0.9712$ ms. And when the batch verification is implemented, $(n + 2)$ scale multiplications, $(3n - 1)$ point additions and $(2n)$ one-way hash functions are performed, which is $(n + 2)T_m + (3n - 1)T_a + (2n)T_h \approx (0.331n + 0.6412)$ ms.

In the scheme of Li et al. [24] (EPA-CPPA), to sign a single message, one scale multiplication and two one-way hash functions are required, which is $1T_m + 2T_h \approx 0.3238$ ms. When to verify a single message, it costs four scale multiplications, one point addition and two one-way hash functions, which is $4T_m + 1T_a + 2T_h \approx 1.2916$ ms. And when the batch verification is implemented, $(2n + 2)$ scale multiplications, (n) point additions and $(2n)$ one-way hash functions are performed, which is $(2n + 2)T_m + (n)T_a + (2n)T_h \approx (0.648n + 0.6436)$ ms.

In the scheme of Li et al. [45], to sign a single message, one scale multiplication and one one-way hash function are required, which is $1T_m + 1T_h \approx 0.3228$ ms. When to verify a single message, it costs three scale multiplications, three point additions and two one-way hash functions, which is $3T_m + 3T_a + 2T_h \approx 0.9746$ ms. And when the batch verification is implemented, $(n + 2)$ scale multiplications, $(3n)$ point additions and $(2n)$ one-way hash functions are performed, which is $(n + 2)T_m + (3n)T_a + (2n)T_h \approx (0.331n + 0.6436)$ ms.

In the proposed scheme, to sign a single message, one scale multiplication and two one-way hash functions are required, which is $1T_m + 2T_h \approx 0.3238$ ms. When to verify a single message, it costs one scale multiplication, one point addition and two one-way hash functions, which is $T_m + T_a + 2T_h \approx 0.3262$ ms. And when the batch verification is implemented, (n) scale multiplications, (n) point additions and $(2n)$ one-way hash functions are performed, which is $(n)T_m + (n)T_a + (2n)T_h \approx (0.3262n)$ ms. The overall overhead is shown in Table 3.

According to Fig. 4, our scheme shows obvious overhead advantages in terms of signing and verifying a single

message. As shown in Fig. 5, our scheme costs the minimum time to batch verify messages among four schemes.

Conclusion

In this paper, a weight-based conditional privacy-preserving authentication scheme in SDVNs is introduced. With this scheme, a secure way to protect the privacy of vehicles and communications between them is offered. By applying the weight-based system, the participation rate of malicious vehicles and communication redundancy are both reduced to ease the computing overhead of entities, which also keeps the communication environment for vehicles clear. The two-step tracing scheme means LCs do not need to store old parameters to obtain the identities of vehicles, thereby reducing deploying costs. For the next step, we will focus on how to manage the vehicles more efficiently to make full use of the advantages of the decoupled architecture in the environment of SDVNs.

Acknowledgements

The authors are very grateful to the anonymous referees for their detailed comments and suggestions regarding this paper.

Authors' contributions

In this work, the idea and overall plan is proposed by Hong Zhong; the concrete cryptographic protocol is conceived and designed by Yingxue Geng; the experiments are performed by Jie Cui and the experimental/analysis tools are contributed by Yan Xu; Lu Liu analyses the collected experimental data.

Authors' information

Hong Zhong was born in Anhui Province, China, in 1965. She received her PhD degree in computer science from University of Science and Technology of China in 2005. She is currently a professor and Ph.D. supervisor of the School of Computer Science and Technology at Anhui University. Her research interests include applied cryptography, IoT security, vehicular ad hoc network, cloud computing security and software-defined networking (SDN). She has over 120 scientific publications in reputable journals (e.g. IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Vehicular Technology, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Network and Service Management, IEEE Transactions on Big Data and IEEE Internet of Things Journal), academic books and international conferences.

Yingxue Geng is now a research student in the School of Computer Science and Technology, Anhui University. Her research focuses on the secure authentication of vehicular ad hoc networks.

Jie Cui was born in Henan Province, China, in 1980. He received his Ph.D. degree in University of Science and Technology of China in 2012. He is currently a professor and Ph.D. supervisor of the School of Computer Science and Technology at Anhui University. His current research interests include applied cryptography, IoT security, vehicular ad hoc network, cloud computing security and software-defined networking (SDN). He has over 100 scientific publications in reputable journals (e.g. *IEEE Transactions on Dependable and Secure Computing*, *IEEE Transactions on Information Forensics and Security*, *IEEE Journal on Selected Areas in Communications*, *IEEE Transactions on Vehicular Technology*, *IEEE Transactions on Intelligent Transportation Systems*, *IEEE Transactions on Multimedia*, *IEEE Transactions on Network and Service Management*, *IEEE Transactions on Emerging Topics in Computing* and *IEEE Transactions on Circuits and Systems*), academic books and international conferences.

Yan Xu is currently an associate professor of School of Computer Science and Technology at Anhui University. She received the BS and MS degrees from Shandong University in 2004 and 2007, respectively, and the PhD degree from University of Science and Technology of China in 2015. Her research interests include information security and applied cryptography.

Lu Liu is the Professor of Informatics and Head of School of Informatics in the University of Leicester, UK. Prof Liu received the Ph.D. degree from University of Surrey, UK and MSc in Data Communication Systems from Brunel University, UK. Prof Liu's research interests are in areas of cloud computing, service computing, computer networks and peer-to-peer networking. He is a Fellow of British Computer Society (BCS).

Funding

The work was supported by the National Natural Science Foundation of China (No. 61872001, No. 62011530046, No. U1936220), the Cooperation and Exchange Project between NSFC and RFBR (No. 20-57-53019, No. 62011530046), the Open Fund of Key Laboratory of Embedded System and Service Computing (Tongji University), Ministry of Education (No. ESSCKF2018-03), the Open Fund for Discipline Construction, Institute of Physical Science and Information Technology, Anhui University and the Excellent Talent Project of Anhui University.

Availability of data and materials

Data supporting the results of this article have been included within the article.

Competing interests

The authors declare that they have no competing interests.

Author details

¹School of Computer Science and Technology, Anhui University, Jiulong Road, 230039 Hefei, China. ²School of Informatics, University of Leicester, University Road, LE1 7RH Leicester, UK.

Received: 8 June 2020 Accepted: 8 September 2020

Published online: 23 September 2020

References

1. Ma X, Gao H, Xu H, Bian M (2019) An IoT-based task scheduling optimization scheme considering the deadline and cost-aware scientific workflow for cloud computing. *EURASIP J Wirel Commun Netw* 2019(1):249
2. Gao H, Xu Y, Yin Y, Zhang W, Li R, Wang X (2019) Context-aware QoS prediction with neural collaborative filtering for Internet-of-Things services. *IEEE Internet of Things J* 7(5):4532–4542
3. Deng S, Xiang Z, Zhao P, Taheri J, Gao H, Yin J, Zomaya A (2020) Dynamical resource allocation in edge for trustable Internet-of-Things systems: a reinforcement learning method. *IEEE Trans Ind Inform* 16(9):6103–6113
4. Gao H, Duan Y, Shao L, Sun X (2019) Transformation-based processing of typed resources for multimedia sources in the IoT environment. *Wirel Netw*:1–17. <https://doi.org/10.1007/s11276-019-02200-6>
5. Lai C, Lu R, Zheng D, Shen XS (2020) Security and privacy challenges in 5G-enabled vehicular networks. *IEEE Network* 34(2):37–45
6. Wang M, Liu D, Zhu L, Xu Y, Wang F (2016) LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication. *Computing* 98(7):685–708
7. Cheng J, Yuan G, Zhou M, Gao S, Liu C, Duan H, Zeng Q (2020) Accessibility analysis and modeling for IoV in an urban scene. *IEEE Trans Veh Technol* 69(4):4246–4256
8. Cheng J, Yuan G, Zhou M, Gao S, Liu C, Duan H (2019) A fluid mechanics-based data flow model to estimate VANET capacity. *IEEE Trans Intell Transp Syst* 21(6):2603–2614
9. Lai C, Zhang K, Cheng N, Li H, Shen X (2016) SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs. *IEEE Trans Intell Transp Syst* 18(6):1559–1574
10. Li H, Dong M, Ota K (2016) Control plane optimization in software-defined vehicular ad hoc networks. *IEEE Trans Veh Technol* 65(10):7895–7904
11. He D, Zeadally S, Xu B, Huang X (2015) An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Trans Inf Forensics Secur* 10(12):2681–2691
12. Cui J, Zhang X, Zhong H, Zhang J, Liu L (2019) Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment. *IEEE Trans Inf Forensics Secur* 15:1654–1667
13. Zhu M, Cao J, Pang D, He Z, Xu M (2015) SDN-based routing for efficient message propagation in VANET. In: *International Conference on Wireless Algorithms, Systems, and Applications*, Springer. pp 788–797
14. Cui J, Wei L, Zhong H, Zhang J, Xu Y, Liu L (2020) Edge computing in VANETs-an efficient and privacy-preserving cooperative downloading scheme. *IEEE J Sel Areas Commun* 38(6):1191–1204
15. Chen M, Qian Y, Mao S, Tang W, Yang X (2016) Software-defined mobile networks security. *Mob Netw Appl* 21(5):729–743
16. Jaballah WB, Conti M, Lal C (2019) A survey on software-defined VANETs: benefits, challenges, and future directions. *arXiv 1904.04577*
17. Cheng J, Chen M, Zhou M, Gao S, Liu C, Liu C (2018) Overlapping community change point detection in an evolving network. *IEEE Trans Big Data* 6:189–200
18. Pentikousis K, Wang Y, Hu W (2013) Mobileflow: Toward software-defined mobile networks. *IEEE Commun Mag* 51(7):44–53
19. Liyanage M, Gurtov A, Ylianttila M (2015) *Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture*. John Wiley & Sons
20. Liyanage M, Ylianttila M, Gurtov A (2014) Securing the control channel of software-defined mobile networks. In: *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, IEEE. pp 1–6
21. Bousselham M, Abdellaoui A, Chaoui H (2017) Security against malicious node in the vehicular cloud computing using a software-defined networking architecture. In: *2017 International Conference on Soft Computing and Its Engineering Applications (icSoftComp)*, IEEE. pp 1–5
22. Azees M, Vijayakumar P, Deboarh LJ (2017) EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. *IEEE Trans Intell Transp Syst* 18(9):2467–2476
23. Lu R, Lin X, Zhu H, Ho PH, Shen X (2008) ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In: *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, IEEE. pp 1229–1237
24. Li J, Choo KKR, Zhang W, Kumari S, Rodrigues JJ, Khan MK, Hogrefe D (2018) EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *Veh Commun* 13:104–113
25. Cui J, Wu D, Zhang J, Xu Y, Zhong H (2019) An efficient authentication scheme based on semi-trusted authority in VANETs. *IEEE Trans Veh Technol* 68(3):2972–2986
26. Cui J, Zhang J, Zhong H, Xu Y (2017) SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter. *IEEE Trans Veh Technol* 66(11):10283–10295
27. Sun Y, Lu R, Lin X, Shen X, Su J (2010) An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. *IEEE Trans Veh Technol* 59(7):3589–3603
28. Hamdoun S, Rachedi A, Ghamridoudane Y (2020) Graph-based radio resource sharing schemes for MTC in D2D-based 5G networks. *Mob Netw Appl*:1–19
29. Duan P, Peng C, Zhu Q, Shi J, Cai H (2014) Design and analysis of software defined vehicular cyber physical systems. In: *2014 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS)*, IEEE. pp 412–417
30. Kim M, Jang I, Choo S, Pack S (2016) On security in software-defined vehicular cloud. In: *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, IEEE. pp 1259–1260

31. Lu R, Lin X, Shi Z, Shen XS (2013) A lightweight conditional privacy-preservation protocol for vehicular traffic-monitoring systems. *IEEE Intell Syst* 28(3):62–65
32. Lo N-W, Tsai J-L (2015) An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. *IEEE Trans Intell Transp Syst* 17(5):1319–1328
33. Gao H, Miao H, Liu L, Kai J, Zhao K (2018) *Int J Softw Eng Knowl Eng* 28(10):1369–1397
34. Shao J, Lin X, Lu R, Zuo C (2015) A threshold anonymous authentication protocol for VANETs. *IEEE Trans Veh Technol* 65(3):1711–1720
35. Lai C, Zhou H, Cheng N, Shen XS (2017) Secure group communications in vehicular networks: A software-defined network-enabled architecture and solution. *IEEE Veh Technol Mag* 12(4):40–49
36. Lai C, Lu R, Zheng D (2017) Achieving secure and seamless ip communications for group-oriented software defined vehicular networks. In: *International Conference on Wireless Algorithms, Systems, and Applications*, Springer. pp 356–368
37. Cui J, Zhang X, Zhong H, Ying Z, Liu L (2019) RSMA: Reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks. *IEEE Internet of Things J* 6(4):6417–6428
38. Zhang J, Cui J, Zhong H, Chen Z, Liu L (2019) PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. *IEEE Trans Dependable and Secure Comput*. <https://doi.org/10.1109/TDSC.2019.2904274>
39. Garg S, Kaur K, Kaddoum G, Ahmed SH, Jayakody DNK (2019) SDN-based secure and privacy-preserving scheme for vehicular networks: A 5G perspective. *IEEE Trans Veh Technol* 68(9):8421–8434
40. Huang J, Qian Y, Hu RQ (2020) Secure and efficient privacy-preserving authentication scheme for 5G software defined vehicular networks. *IEEE Trans Veh Technol*. <https://doi.org/10.1109/TVT.2020.2996574>
41. Ming Y, Cheng H (2019) Efficient certificateless conditional privacy-preserving authentication scheme in VANETs. *Mob Inf Syst* 2019:1–19
42. Pointcheval D, Stern J (2000) Security arguments for digital signatures and blind signatures. *J Cryptol* 13(3):361–396
43. Cui J, Zuo HF, Zhong H (2017) Asymmetric Biclique cryptanalysis of lightweight block ciphers MIBS and I-PRESENT. *Sci Sin Informationis* 47(10):1395–1410
44. Cui J, Zuo HF, Zhong H (2017) Biclique cryptanalysis on lightweight block ciphers I-PRESENT-80 and I-PRESENT-128. *J Commun* 11:2
45. Li C, Zhang X, Wang H, Li D (2018) An enhanced secure identity-based certificateless public key authentication scheme for vehicular sensor networks. *Sensors* 18(1):194

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Submit your manuscript to a SpringerOpen[®] journal and benefit from:

- Convenient online submission
- Rigorous peer review
- Open access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

Submit your next manuscript at ► [springeropen.com](https://www.springeropen.com)
