A Security-Enhanced Certificateless Aggregate Signature Authentication Protocol for InVANETs

Guangquan Xu, Wenjuan Zhou, Arun Kumar Sangaiah, Yao Zhang, Xi Zheng, Qiang Tang, Naixue Xiong, Kaitai Liang, and Xiaokang Zhou

Abstract

The pervasive communications between vehicles and dynamic mobility may significantly increase data exchange and therefore bring a huge amount of traffic data in InVANETs. Due to some environmental factors, like the vulnerability of wireless connection, limitation of in-car computing ability, and speed of vehicles, it is extremely challenging to design identity authentication protocols satisfying the requirements of both high security and efficiency simultaneously. To this end, the aggregate signature technology has been employed in InVANETs. However, the technology still suffers from high computational overhead due to the management of certificates, as well as the key escrow problem (i.e., the dependence on a fully trusted third party). In this article, we propose the SE-CLASA protocol for InVANETs in order to tackle the aforementioned problems. In addition, a novel factor-contained aggregation mechanism is proposed to resist an information injection attack investigated in our analysis. Moreover, we prove the security of the proposed SE-CLASA and conclude that it meets most known security requirements in a general InVANET scenario. Simulation results show the superiority of the proposed SE-CLASA, in terms of security and efficiency, compared to the most recent authentications in InVANETs.

Introduction

The intelligent vehicular ad hoc network (InVANET) is one of the most promising structures for future intelligent networks, connecting various electronic devices and machines to provide optimized policies for users. In InVANETs, nodes may be all kinds of smart vehicles (e.g., buses, cars, trucks, and motorcycles), which could collect dynamic traffic related messages and communicate with other nodes and the automated communication infrastructures (e.g., roadside units and traffic control centers). Spending time on transportation every day, vehicle users and traffic monitors may expect that InVANETs can help improve traffic safety, control traffic flow, and provide a better driving experience for drivers [1]. Accordingly, the design of InVANETs should focus on providing intelligent transportation services to build harmonious connections between vehicles and people [2].

There are two kinds of communications in an InVANET system, namely vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication. According to the dedicated short-range communication (DSRC) protocol in the wireless communication environment, vehicles broadcast messages about traffic conditions (e.g., weather, road congestion), as well as the vehicle state information (e.g., location, direction, speed, driving status) every 100-300 ms [3]. When receiving the information, other vehicles can adjust their route to avoid traffic jams or accidents. Furthermore, a roadside unit (RSU) can collect the messages and send them to the traffic control center, which can take some timely intelligent actions to improve traffic efficiency and safety by analyzing these messages [4]. For example, by collecting and analyzing a large number of real-time messages, the traffic control center can foresee road congestion ahead of time and calculate the optimal route for drivers. We can achieve intelligent road traffic management by InVANETs and the automated transportation infrastructures.

Identity authentication is a significant requirement to guarantee trust in communication, especially when an RSU is ready to receive messages from other vehicles in InVANETs. The V2I authentication process requires vehicles to sign messages; then intelligent communication infrastructure verifies signatures. However, in a general InVANETs scenario, vehicles communicate with other entities in wireless surroundings, which may not be secure and the privacy of vehicle users should be protected. Therefore, many anonymous identity authentication schemes are provided to protect the privacy of vehicle users [5–8]. Moreover, due to high-speed movement and a large number of waiting nodes in a metropolitan-area, an authentication process should be as short as possible to satisfy the stringent time requirement [9, 10].

In practice, we have to be concerned about both the security and privacy problems in InVANETs. In terms of security, due to the wireless communication, adversaries can modify, intercept, or delete any messages transmitted in InVANETs. Therefore, a receiver (a vehicle or an RSU) must check the message integrity and the sender's identity beforehand because the original messages may be modified by adversaries, which may result in information misinterpretation that yields convenience or even endangers driver safety. For

Guangquan Xu is with Jiangsu University of Technology and Tianjin University; Wenjuan Zhou, Yao Zhang and Naixue Xiong (corresponding author) are with Tianjin University; Arun Kumar Sangaiah is with Vellore Institute of Technology (VIT); Xi Zheng is with Macquarie University; Qiang Tang is with the New Jersey Institute of Technology; Kaitai Liang is with the University of Surrey; Xiaokang Zhou is with Shiga University.

Digital Object Identifier:
10.1109/MNET.001.1900035

0890-8044/20/$25.00 © 2020 IEEE

instance, an adversary may send road congestion messages intensively so that other vehicles have to keep re-routing according to incorrect information, which will lead to unnecessary waste of time.

For privacy, adversaries may capture the traveling route of a certain vehicle by analyzing the vehicle's broadcast messages. It is an infringement of driver privacy. Greater danger may be yielded if these traveling routes are shared to commit crimes. Therefore, the anonymity technology should be introduced to safeguard the privacy of drivers in InVANETs. However, there are still some challenges in anonymity: once an adversary has an anonymous identity, he/she can release malicious messages unscrupulously, and no one can extract his/her real identity. This is very dangerous for intelligent transportation systems. Therefore, traceability and unlinkability are two important features because the trusted authority should have the ability to reveal a vehicle's real identity from communications, and any other vehicles cannot infer a vehicle's real identity by analyzing its sending messages. This may be useful in the case where a driver may be malicious, for example, when a malicious vehicle broadcasts an incorrect message, which will lead to accidents or crimes. In such a case, the driver should be identified and punished by law [5].

In order to tackle the security and privacy issues in InVANETs, several conditional privacy preserving protocols have been proposed. The traditional public key infrastructure (PKI)-based authentication turns out to be a surprisingly intricate and resource-intensive approach, because a large number of certificates must be managed and transformed along with authentication messages.

Identity-based (IDB) cryptography is a promising technology in the authentication of InVANETs, which could overcome the shortcomings of the PKI-based schemes [5, 11]. In the IDB authentication schemes, a user's public key can easily be calculated by their identity, such as an email address or a telephone number, while a trusted third party called a private key generator computes the corresponding private key and sends it to the user secretly. Therefore, the IDB scheme avoids using certificates in the signature authentication phase, which can reduce the additional overhead of managing a large number of certificates. However, the IDB schemes are only fit for private networks due to the key escrow problem, which means that all vehicles must fully trust the private key generator. This assumption may be too strong for a public network.

In order to solve the inherent key escrow problem in IDB cryptography, the concept of certificateless public key cryptography (CL-PKC) is proposed, in which no certificates are needed to ensure the authenticity of public keys either [12]. In CL-PKC, a trusted third-party key generation center (KGC) helps a vehicle generate his/her private key. However, the vehicle's full private key cannot be accessed by the KGC, which only provides a vehicle with a partial signing key. The vehicle generates his/her full signing key by combining the partial signing key with their selected secret values.

In recent years, CL-PKC-based certificateless aggregate signature (CLAS) authentication protocols have been introduced to improve the efficiency of signature authentication [6–8]. The aggregation algorithm in an aggregate signature can aggregate *n* signatures on *n* distinct messages from *n* distinct users into a single short signature. This technique can reduce signature length and hence reduce the verification cost, especially in resource-constrained environments. However, there are some drawbacks in the current CLAS authentication protocols, which are described as follows:

- The general CL-PKC-based signature schemes are not applicable to the InVANETs scenario, in which users broadcast messages with pseudo identities in plaintext, so message secrecy is not considered. Therefore, the user's public/private key pair generation phase in the CL-PKC is redundant.
- The traditional CLAS authentication protocols cannot resist the information injection attack in signature aggregation, in which attackers could muddle through the aggregate signature verification by playing tricks on several valid signatures.
- Most of the traditional CLAS authentication protocols are designed based on bilinear pairings, which will bring expensive computational overhead.

Research Contributions

To achieve high dependability and low computation cost for InVANETs, a security-enhanced certificateless aggregate signature authentication (SE-CLASA) protocol is presented in this article. The main contributions of our work are as follows:

- We propose a security-enhanced certificateless aggregate signature authentication protocol, which is more efficient and suitable for V2I communication in InVANETs (note that there is no need to generate the vehicle's private/public key pair in our protocol).
- We present a factor-contained aggregate signature mechanism for our SE-CLASA, which can prevent the information injection attack in the signature aggregation phase.
- We optimize the computation and communication overhead of our scheme to make them acceptable compared to the state-of-the-art schemes.

Preliminaries

In this section, we describe the design goals and cryptography basis (elliptic curve cryptography) of our SE-CLASA protocol.

Design Goals

In order to satisfy the security and privacy requirements in InVANETs, as well as achieve high efficiency in computation and communication cost, an SE-CLASA protocol should have the following properties.

Message Authentication: Once an RSU receives a message, it should have the ability to verify the legitimacy of the sender and data consistency without being modified by others [13].

Privacy Preservation: In InVANETs, vehicles should stay anonymous with each other, and no other RSUs or vehicles can infer the real identity of a vehicle by analyzing a number of messages sent by the vehicle.

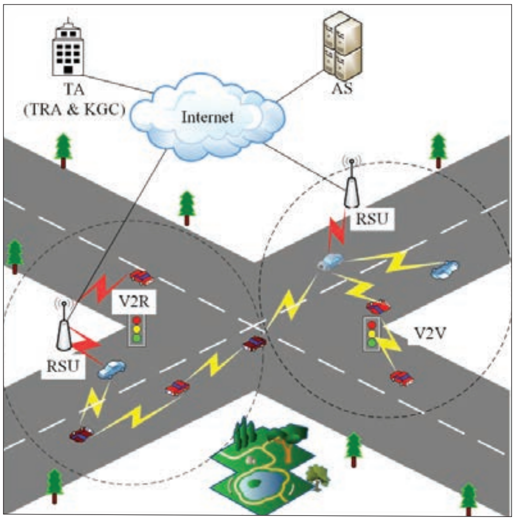

FIGURE 1. The network model of InVANETs.

Traceability: Although a vehicle's real identity is invisible to other vehicles, the TRA must have the ability to recover it from the corresponding pseudo identity when the signature is in dispute.

Unlinkability: This is to prevent malicious vehicles in the system linking two messages sent by the same vehicle. For example, the attacker cannot infer a vehicle's route by analyzing his sending messages.

High Efficiency: To adapt to the resource-constrained environment of InVANETs, we should employ lightweight cryptographic algorithms (e.g., Map-to-Point and bilinear pairing operations) to improve the time efficiency of the protocol.

Resistance to Attacks: Our proposed SE-CLASA protocol can resist an information injection attack occurring in the signature aggregation phase. In this attack, adversaries can muddle through the aggregate verification by tampering with several valid signatures. We show details in the discussion section.

Cryptography Basis

Elliptic curve cryptography (ECC) is an algorithm for establishing public key encryption. Its security relies on the widely recognized difficulty in solving elliptic curve discrete logarithm problems. It is widely used in designing digital signature protocols due to its high security, low consumption, and fast computing speed (a 163-bit ECC password strength is approximately equivalent to 1024-bit RSA password strength).

An SE-CLASA Protocol

In this section, we first introduce the network model of InVANETs and our SE-CLASA protocol overview. After that, we introduce the services of our protocol, which contains four phases: system initialization, pseudo identity generation, message signing, and signature aggregation and verification. In addition, a factor-contained aggregate signature mechanism could provide superior security protection in the signature verification phase.

Network Model

We define a two-layer vehicular network model, much like [5]. Figure 1 shows the main components of the network model. The upper layer is composed of the application servers (ASs, e.g., a traffic management center) and the trust authorities (TAs). In our protocol, the Key Generation Center (KGC) and the Trace Authority (TRA) play the part of TA together. The TAs take charge of system parameters initialization, and then preload them to an onboard unit (OBU), which is a wireless communication device embedded in a vehicle. The AS is an intelligent communication infrastructure responsible for collecting traffic-related messages from RSUs and taking further actions for the intelligent transportation system. The upper layer entities and RSUs communicate with each other through secure transmission protocols, such as the wired Transport Layer Security protocol. The bottom layer consists of vehicles and RSUs, and they communicate with one another through the DSRC protocol. The RSUs fixed on the roadside can check the messages' validity and transmit the valid messages to the AS or deal with it locally. The vehicle could send safety messages to the nearby RSU using an OBU.

SE-CLASA Overview

In order to satisfy the conditional privacy preservation in InVANETs, we introduce a pseudo identity for each vehicle, and only the trust authority can convert the vehicle's real identity from its pseudo identity. The main participants of the authentication process and their characteristics are illustrated as follows.

Trust Authority: A TA is a trusted third party with high computational capability. It is in charge of initializing the system parameters (e.g., public keys of the TRA and the KGC and the definition of the eclipse curve) and sending them to the OBU of each vehicle. In our SE-CLASA protocol, there are two trusted parties. The KGC is responsible for generating a vehicle's pseudo identity, and the TRA is responsible for extracting the real identity of a vehicle from the broadcast messages.

Application Server: An AS could provide some value-added services (e.g., personalized advertisement and entertainment recommendations) by collecting and analyzing vast amounts of traffic related messages from RSUs.

Roadside unit: RSUs are wireless communication device distributed evenly or unevenly along the roadside. The computational capability is lower than that of the TA and higher than that of the vehicle. An RSU is able to verify the validation of the signature in a received message and transmit it to the AS or the traffic management center for further studies.

Vehicle: Vehicles are the moving nodes in InVANETs. A vehicle has the lowest computational capability. A wireless communication device (OBU) is embedded in the vehicle, and it helps the vehicle communicate with other vehicles and RSUs. Each vehicle maintains a pseudo identity pool, and every time it signs a message, a pseudo identity is selected to transmit with it.

SE-CLASA Services

In this subsection, we introduce the process of system initialization pseudo identity generation, message signing, and signature aggregation and verification. The details of each process are shown in Fig. 2.

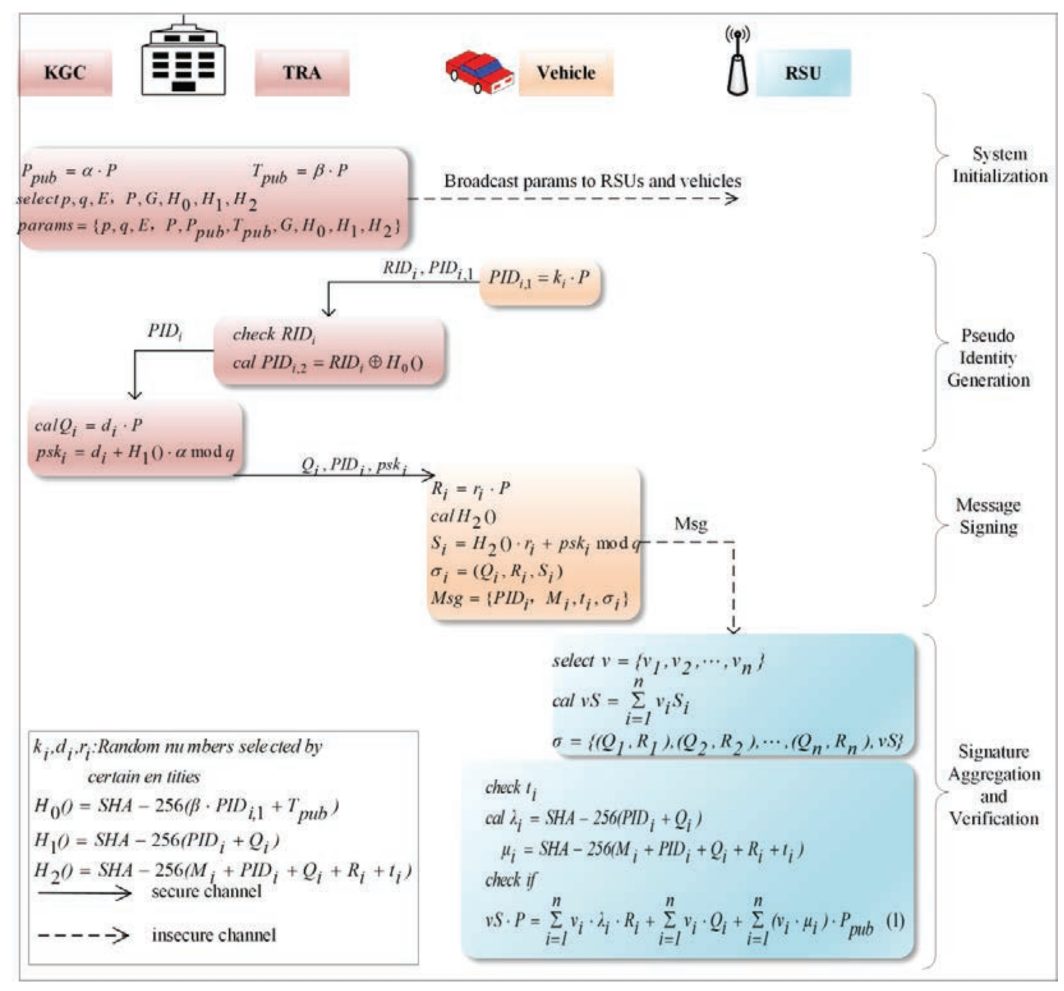
KGC
TRA
Vehicle
RSU
$P_{pub} = \alpha \cdot P$
$T_{pub} = \beta \cdot P$
select $p, q, E, P, G, H_0, H_1, H_2$
params $= \{p, q, E, P, P_{pub}, T_{pub}, G, H_0, H_1, H_2\}$
Broadcast params to RSUs and vehicles
System Initialization
$RID_i, PID_{i,1}$
$PID_{i,1} = k_i \cdot P$
PID_i
check RID_i
cal $PID_{i,2} = RID_i \oplus H_0()$
Pseudo Identity Generation
cal $Q_i = d_i \cdot P$
$psk_i = d_i + H_1() \cdot \alpha \bmod q$
Q_i, PID_i, psk_i
$R_i = r_i \cdot P$
cal $H_2()$
$S_i = H_2() \cdot r_i + psk_i \bmod q$
$\sigma_i = (Q_i, R_i, S_i)$
$Msg = \{PID_i, M_i, t_i, \sigma_i\}$
Msg
Message Signing
select $v = \{v_1, v_2, \cdots, v_n\}$
cal $vS = \sum_{i=1}^{n} v_i S_i$
$\sigma = \{(Q_1, R_1), (Q_2, R_2), \cdots, (Q_n, R_n), vS\}$
check t_i
cal $\lambda_i = SHA-256(PID_i + Q_i)$
$\mu_i = SHA-256(M_i + PID_i + Q_i + R_i + t_i)$
check if
$vS \cdot P = \sum_{i=1}^{n} v_i \cdot \lambda_i \cdot R_i + \sum_{i=1}^{n} v_i \cdot Q_i + \sum_{i=1}^{n} (v_i \cdot \mu_i) \cdot P_{pub}$ (1)
Signature Aggregation and Verification
k_i, d_i, r_i: Random nu mbers sele cted by certain en tities
$H_0() = SHA-256(\beta \cdot PID_{i,1} + T_{pub})$
$H_1() = SHA-256(PID_i + Q_i)$
$H_2() = SHA-256(M_i + PID_i + Q_i + R_i + t_i)$
secure channel
insecure channel

FIGURE 2. The process of SE-CLASA.

System initialization: In this phase, two TAs, a KGC, and a TRA generate system parameters for every vehicle and RSU as follows:

- The TAs select two large prime numbers p, q and a non-singular elliptic curve E. Let G be a finite cyclic group of order q, and TAs select a point P on E as its generator.
- The KGC selects a random number a as its private key and calculates the corresponding public key P_{pub}. The private key, which is used for partial signing key generation, is kept secret by the KGC.
- The TRA selects a random number β as its private key and calculates the corresponding public key T_{pub}. The private key, which is used for traceability, is kept secret by the TRA.
- The TAs use the hash algorithm to transfer three hash values and H_0, H_1, and H_2. We employ the SHA-256 algorithm in our protocol. Then the TAs broadcast these public system parameters to all the vehicles and RSUs.

Pseudo Identity Generation: When vehicles first join InVANETs, they have to request TAs for identity authentication by means of sending their real identities (RIDs) to the TRA. A RID can inimitably identify the vehicle like a license plate number or an identity number. The TRA verifies the validity of a vehicle's RID first and then generates a pseudo identity PID_i for each vehicle (PID_i consists of two parts, $PID_{i,1}$ and $PID_{i,2}$). Only the TRA can extract a RID from its PID. We explain the process of pseudo identity generation as follows.

- The vehicle sends his/her RID and $PID_{i,1}$ to the TRA through a secure channel. $PID_{i,1}$ is a part of PID_i, which contains some random numbers selected by the vehicle.
- When the TRA receives the message, it checks the validity of the RID first. Then the TRA calculates $PID_{i,2}$ through an XOR operation, which is performed on RID_i and a hash value $H_0()$. After that, $PID_{i,1}$ and $PID_{i,2}$ constitute a pseudo identity PID_i for the vehicle, which will be sent to the KGC through a secure channel. According to the characteristic of the XOR, only the TRA who knows its own private key can extract a vehicle's RID from its PID.
- When the KGC receives PID_i, it calculates a parameter Q_i using its own selected random number. Then it sets up a partial signing key (psk_i) for the vehicle, which is used to sign a message later in the message signing phase. Finally, the KGC sends Q_i, PID_i, and psk_i to the vehicle through a secure channel.

Specifically, we preload a pool of pseudo identities and partial signing keys to the vehicle to protect the vehicle's privacy. The pseudo identities with short valid periods are refilled through the pseudo identity generation algorithm when the network is not busy.

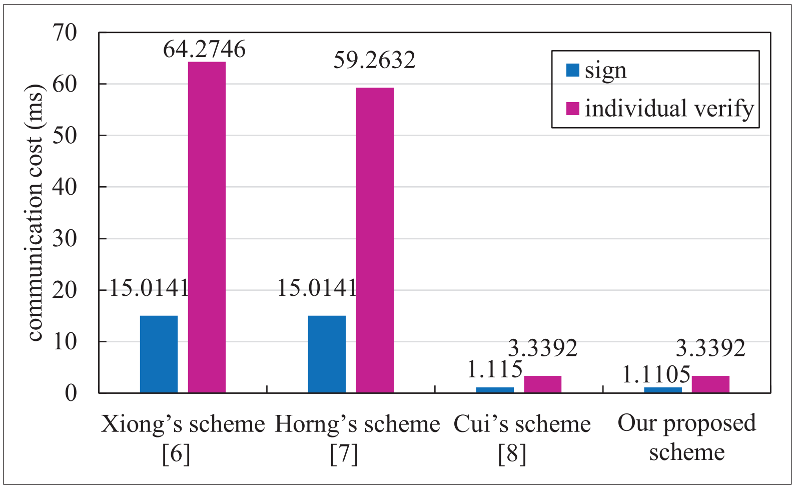

FIGURE 3. Computation cost of sign and individual verify algorithm.

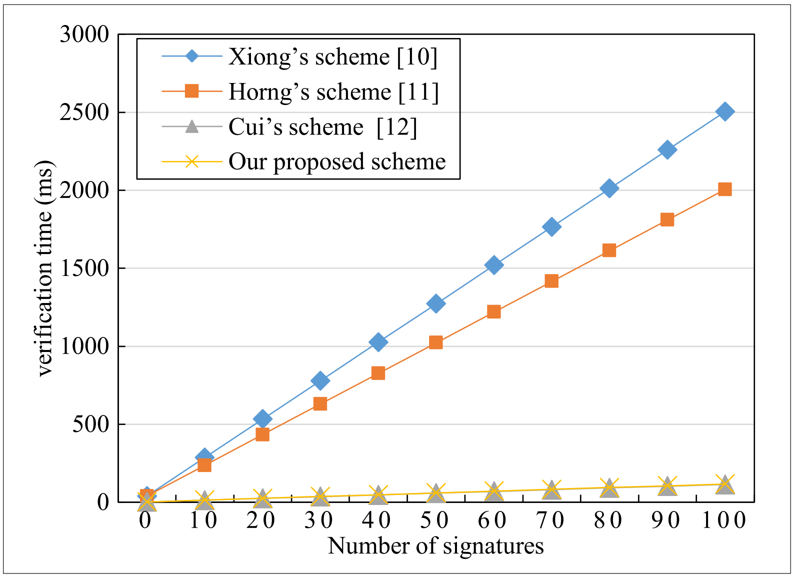

FIGURE 4. Verification delay vs. number of signatures in CLAS schemes.

Message Signing: in InVANETs, every message sent by a vehicle has to be verified, which can ensure message integrity and authentication. A vehicle first takes out a PID from its storage randomly. Then it utilizes the combination of its own secret numbers and psk_i to sign a message. Specifically, the vehicle executes the following steps in this phase.

- The vehicle calculates a parameter R_i by use of its selected random number.
- It makes a hash function over the traffic related message M_i, PID_i, the parameter R_i, Q_i, and the current timestamp t_i to guarantee the message integrity, which is transmitted through an insecure channel.
- It calculates a parameter S_i by using its own secret numbers and psk_i, and constructs a signature s_i on M_i.
- The vehicle broadcasts the *Msg* to the InVANETs.

These steps are repeated every 100–300 ms. As is known, the parameter R_i calculated by the vehicle and the psk_i calculated by the KGC make up the full secret key to sign a message. Therefore, we can solve the key escrow problem perfectly, because the KGC cannot counterfeit a legal digital signature on a certain message on its own.

Signature Aggregation and Verification: The aggregate signature generator can aggregate a large number of signatures and verify them at the same time. The RSU plays the role of the aggregate signature generator in our protocol. We illustrate the process of signature aggregation and verification as follows:

- When the RSU receives multiple broadcast messages that are sent by different vehicles, it first generates a vector consisting of small random integers. The vector is used to resist the information injection attack of the aggregated signatures. Then the RSU computes a factor-contained certificateless aggregate signature σ.
- Using the public parameters and other messages received from the vehicles, the RSU first checks the freshness of the timestamp of each message; if it is not within a certain time period, the RSU rejects the message.
- Then the RSU calculates two hash values, λ_i and μ_i, for each message. According to the characteristic of hash function, if the parameters (M_i, PID_i, Q_i, etc.) are not modified during transfer, the value of l_i and m_i are equal to $H_1()$ and $H_2()$, respectively.
- Finally, the RSU checks if Eq. 1 in Fig. 2 is true to verify the validation of signatures in bulk. Based on the previous description, only if each signature is valid can the equation be established.

When the signatures are identified to be valid, the RSU can resend them to the vehicles to optimize their driving routes. Compared to the method of verifying the messages one by one, the aggregate method can not only reduce the length of the signature, but also alleviate the computational overhead. Moreover, only several general hash functions and XOR operations are required in our protocol, which requires less computation cost than protocols using bilinear pairing operations.

Performance Evaluation

In this section, the computational cost of our SE-CLASA protocol is evaluated first; we select three most recent CLAS authentication protocols to make a comparison. Next, we compare the performance of our SE-CLASA protocol with four other InVANET-based authentication protocols.

In our experiment, we use a personal computer (HP with an Intel I5-6500 3.20 GHz processor, 8 GB memory, and Windows 10) to calculate the running time of the operations used in our SE-CLAS protocol and the compared CLAS authentication protocols. The operations include the bilinear pairing operation (bp), the bilinear pairing-based scale multiplication operation (bp-mul), the bilinear pairing-based point addition operation (bp-add), and the Map-to-Point operation (mtp) used in the other protocols. As well as the scale multiplication operation based on ECC (ecc-mul), the addition operation based on ECC (ecc-add), and the generation hash function SHA-256 (H) appeared in our SE-CLASA protocol. We evaluate the verification time of the RSU by measuring execution time of each operation. We executed the experiment

100 times to get the average running time by use of the PyECC library and the python-ate-bilinear-pairing 0.6 library.

Comparison of Traditional CLAS Protocols

We compare the computational cost of our proposed SE-CLASA protocol with the most recent CLAS authentication protocols [6–8].

Figure 3 shows the results intuitively for the running time in message signing and individual verification. We can get that in the message signing algorithm; our protocol has 92.60 percent improved performance over those of Xiong *et al.*,'s protocol [6] and Horng *et al.*,'s protocol [6], and we have the same computation cost with Cui *et al.*'s protocol [8]. In addition, in the individual verify algorithm, our proposed SE-CLASA protocol has 94.88 and 94.45 percent improved performance over those of Xiong *et al.*'s protocol and Horng *et al.*'s protocol, respectively.

Figure 4 shows the results for the running time in verifying a collection of aggregated signatures. It is clear that our proposed SE-CLASA protocol has lower verification delay compared to the protocols in [6, 7]. Although we have almost the same verification delay as the protocol in [8], our proposed SE-CLASA protocol can resist the information injection attack in the aggregate signature verification phase, which is more secure compared to Cui *et al.*'s protocol. It is worth sacrificing a bit of computation cost for security within an acceptable range, since security is the most important issue in practical applications.

Comparison of InVANET-Based Protocols

In order to satisfy the security and privacy preservation requirements, a variety of InVANET-based authentication protocols have been proposed [5, 11, 14, 15]. In [15], Horng *et al.* proposed a batch verification scheme for V2V communication, which is called batch verification for secure and privacy enhancing communication scheme (b-SPECS+). In [15], a group communication protocol was proposed, in which vehicles can authenticate and communicate with one another. By using batch verification, the signature verification speed improved a lot.

In [5], He *et al*. introduced an identity-based conditional privacy-preserving authentication protocol (CPPA) that combines the technology of group signature and pseudonym authentication. Their scheme is much more efficient in computation cost than many other schemes [11, 14, 15]. However, in their scheme, the private key of a system is pre-loaded in the vehicle's tamper-proof device, which can be taken out by attackers (e.g., through side channel attacks). Therefore, their solution is not secure when the attackers have physical access to the tamper-proof device.

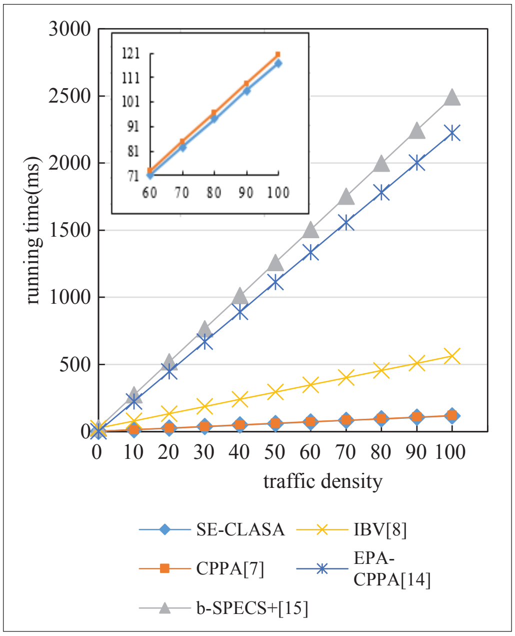

FIGURE 5. Verification delay vs. traffic density in VANET-based schemes.

Figure 5 displays the tendency of verification delay with the increase of the number of vehicles within the domination area of an RSU. The small figure embedded in Fig. 5 is a magnified image of the proposed SE-CLASA protocol and the CPPA protocol in [5]. It is clear that our SE-CLASA protocol has much less verification delay than the other protocols. We can see that the number of signatures an RSU can verify in 300 ms is approximately 11, 51, 134, 252, and 260 when b-SPECS+ [15], IBV [11], EPA-CPPA [14], CPPA [5], and our SE-CLASA protocol are proposed, respectively. This means that when the number of verifying signatures goes beyond the maximal thresholds, some signatures would be dropped. Consequently, when the traffic load increases, the proposed SE-CLASA protocol has the ability to verify the maximum number of messages of all the protocols mentioned here.

Discussions

In this section, a comparison of the security and privacy properties is made among our SE-CLASA and the existing protocols [5–8, 11, 14, 15]. Table 1 shows the details of the capacity of message authentication, privacy preservation, traceability, unlinkability, high efficiency, and resistance to information injection attack among the SE-CLASA and the other protocols.

Message Authentication: All the protocols provide message authentication in our comparison list. In our SE-CLASA protocol, according to the aforementioned signature aggregation and verification phase in the protocol, an RSU can check the authentication of the message by verifying the signature.

Privacy Preservation: In the pseudo identity generation phase, the TRA hides the vehicle's real identity in $PID_{i,2}$ through an XOR operation. In order to reveal the real identity from $PID_{i,2}$, an adversary needs to access the TRA's private key. However, the TRA generates its public/private key pairs on the basis of an ECC; hence, it is difficult to access its private key from the corresponding public key. Therefore, the proposed SE-CLASA protocol for InVANETs could achieve privacy preservation.

Traceability: In the pseudo identity generation phase, the vehicle's real identity is contained in $PID_{i,2}$. According to the characteristic of the XOR operation, by knowing the TRA's private key and the public parameter $PID_{i,2}$, the TRA can take out the real identity of the vehicle. Therefore, traceability can be provided in our SE-CLASA protocol.

	[7]	[8]	[10]	[11]	[12]	[14]	[15]	SE-CLASA
Message authentication	✓	✓	✓	✓	✓	✓	✓	✓
Privacy preservation	✓	✓	✓	✓	✓	✓	✓	✓
Traceability	✓	✓	✓	✓	✓	✓	✓	✓
Unlinkability	✓	✓	✓	✓	✓	✓	✓	✓
No bilinear pairing	✓	×	×	×	✓	✓	×	✓
No Map-to-Point	✓	×	×	×	×	×	×	✓
Resistance to information injection attack	×	×	×	×	×	×	×	✓

TABLE 1. A comparison of the previous work and SE-CLASA protocol.

Unlinkability: Each time a message is generated, the KGC and the vehicle will generate three random numbers k_i, d_i,, and r_i separately (the random numbers are introduced in Fig. 2). Due to the randomness of these selected numbers, the adversary cannot connect two pseudo identities or signatures generated by the same vehicle. Moreover, the pseudo identities of the vehicles are changed frequently. Consequently, our proposed SE-CLASA protocol can achieve unlinkability.

High Efficiency: No bilinear pairing and Map-to-Point operations are used in our proposed protocol. Only several general hash functions and XOR operations are required, which makes our protocol more efficient in computation and communication cost.

Resistance to Attacks: In the existing aggregate signature authentication protocols [6, 7, 14], the aggregate signature verification has a leak by which a malicious user can construct bogus signatures and muddle through the aggregate verification. We use a small case to illustrate the information injection attack in the aggregate verification phase. For instance, an adversary intercepts two valid signatures (s1 and s2) and injects *n* and –*n* to s1 and s2, respectively. It is clear that they cannot be detected in the signature aggregate phase because item *n* has been countered by item –*n*. As a consequence, the RSU also cannot detect the injection in the aggregate signature verification phase. In our SE-CLASA protocol, we propose a factor-contained aggregate signature in which a random *n*-dimensional vector **v** is added during the signature aggregation, as shown in Fig. 2. Because of the randomness of the elements in the vector, the information injection attack in the aggregate signature verification phase can be detected by the RSU. Therefore, our proposed SE-CLASA protocol can achieve higher security compared to the existing aggregate signature authentication protocols in InVANETs.

Conclusion and Future Work

In this article, an SE-CLASA protocol for V2I communication in InVANETs is designed based on the CL-PKC technology. There are no public/private key pairs of the vehicles but also no certificates generation phases in our design, which makes the system more efficient, especially in a resource-constrained environment. Moreover, a factor-contained aggregate signature mechanism was proposed to resist the information injection attack in the signature aggregation phase, so the protocol is much more secure than the most recent CLAS authentication protocols. The simulation results and comparison with the state of the art demonstrate that the proposed SE-CLASA protocol is able to provide better security but also achieve significantly greater performance.

Since huge amounts of vehicles will be increasingly used in urban cities, more information exchange among vehicles may be clustered and analyzed in an efficient way. As part of our future work, we will focus on the group management of vehicles in order to further improve the efficiency of data processing, and provide more intelligent and personalized services.

Acknowledgments

This work is partially sponsored by the State Key Development Program of China (no. 2018YFB0804402) and the National Science Foundation of China (no. 61572355, U1736115).

References

[1] M. Muhammad and G. A. Safdar, "Survey on Existing Authentication Issues for Cellular-Assisted V2X Communication," *Vehic. Commun.*, vol. 12, Apr. 2018, pp. 50–65

[2] X. Du *et al.*, "An Effective Key Management Scheme for Heterogeneous Sensor Networks," *Ad Hoc Networks*, vol. 5, no 1, Jan. 2007, pp. 24–34.

[3] S. S. Manvi and S. Tangade, "A Survey on Authentication Schemes in VANETs for Secured Communication," *Vehic. Commun.*, vol. 9, July 2017, pp. 19–30.

[4] H. Ren *et al.*, "Querying in Internet of Things with Privacy Preserving: Challenges, Solutions and Opportunities," *IEEE Network*, vol. 32, no. 6, Nov./Dec. 2018, pp. 144–51.

[5] D. B. He *et al.*, "An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks," *IEEE Trans. Info. Forensics and Security*, vol. 10, no. 12, Dec. 2015, pp. 2681–91.

[6] H. Xiong *et al.*, "An Efficient Certificateless Aggregate Signature With Constant Pairing Computations," *Info. Sciences*, vol. 219, Jan. 2013, pp. 225–35.

[7] S. J. Horng *et al.*, "An Efficient Certificateless Aggregate Signature With Conditional Privacy-Preserving for Vehicular Sensor Networks," *Info. Sciences*, vol. 317, Oct. 2015, pp. 48–66.

[8] J. Cui *et al.*, "An Efficient Certificateless Aggregate Signature Without Pairings for Vehicular Ad Hoc Networks," *Info. Sciences*, vol. 451, July. 2018, pp. 1–15.

[9] X. Du *et al.*, "A Routing-Driven Elliptic Curve Cryptography Based Key Management Scheme for Heterogeneous Sensor Networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, Mar. 2009, pp. 1223–29.

[10] G. Q. Xu *et al.*, "CSP-E2: An Abuse-Free Contract Signing Protocol With Low-Storage TTP for Energy-Efficient Electronic Transaction Ecosystems," *Info. Sciences*, vol. 476, Feb. 2019, pp. 505–15.

[11] S. F. Tzeng *et al.*, "Enhancing Security and Privacy for Identity-Based Batch Verification Scheme in VANETs," *IEEE Trans. Vehic. Tech.*, vol. 66, no. 4, Apr. 2017, pp. 3235–48.

[12] Y. Xiao *et al.*, "A Survey of Key Management Schemes in Wireless Sensor Networks," *J. Computer Commun.*, vol. 30, Sept. 2007, pp. 2314–41.

[13] X. J. Zeng *et al.*, "E-AUA: An Efficient Anonymous User Authentication Protocol for Mobile IoT," *IEEE Internet of Things J.*, June 2018. DOI: 10.1109/JIOT.2018.2847447.

[14] J. L. Li et al., "EPA-CPPA: An Efficient, Provably-Secure and Anonymous Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks," *Vehic. Commun.*, vol. 13, July. 2018, pp. 104–13.

[15] S. J. Horng *et al.*, "b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET," *IEEE Trans. Info. Forensics and Security*, vol. 8, no. 11, Nov. 2013, pp. 1860–75.

Biographies

Guangquan Xu [M'18] (losin@tju.edu.cn) is with the School of Computer Engineering, Jiangsu University of Technology, and the Tianjin Key Laboratory of Advanced Networking (TANK), College of Intelligence and Computing, Tianjin University, China. He received his Ph.D. degree from Tianjin University in March 2008. He is a member of the CCF. His research interests include cyber security and trust management.

Wenjuan Zhou (15849120851@163.com) is a Master's student in the Department of Intelligence and Computing, Tianjin University. She received her B.S. degree from the School of Computer Science and Technology, Inner Mongolia University of China in 2017. Her current research interests include cryptography and security protocols in VANETs.

Arun Kumar Sangaiah [M'15] (arunkumarsangaiah@gmail.com) received his M.Eng. degree from Anna University and his Ph.D. from VIT University, Vellore, India, in 2007 and 2014, respectively. He is currently a professor in the School of Computing Science and Engineering, VIT University. He has been appointed a visiting professor at Southwest Jiaotong University, Chengdu, Changsha University of Science and Technology, China; Dongguan University of Technology, Guangdong; and Hwa-Hsia University of Technology, Taiwan. His areas of research interest include e-Learning, learning engineering, machine learning, software engineering, computational intelligence, IoT, wireless networks, bio-informatics, and embedded systems.

Yao Zhang (zzyy@tju.edu.cn) received his B.S. degree from Hebei University of Economics and Business. He is currently pursuing a Ph.D. degree in the College of Intelligence and Computing, Tianjin University. His current research interests include symbolic execution and program static analysis.

Xi Zheng [M'16] (james.zheng@mq.edu.au) received his Ph.D. in software engineering from the University of Texas, Austin, his Master's degree in computer and information science from the University of New South Wales, and his Bachelor's in computer information systems from FuDan. He is an assistant professor/ lecturer in software engineering at Macquarie University.

Qiang Tang [M'16] (qiang@njit.edu) received his Ph.D from the University of Connecticut and his M.S from the Chinese Academy of Sciences. He is currently an assistant professor in the Computer Science Department of New Jersey Institute of Technology (NJIT), and is also a core member of the NJIT Cybersecurity Research Center. His research interests are blockchain technology, post-Snowden cryptography, copyright protection, and applied crypto and privacy protection in general.

Naixue Xiong [M'06, SM'12] (xiongnaixue@gmail.com) is current a professor in the College of Intelligence and Computing, Tianjin University. He received Ph.D. degrees from both Wuhan University (on sensor system engineering), and the Japan Advanced Institute of Science and Technology (in dependable sensor networks), respectively. His research interests include cloud computing, security and dependability, parallel and distributed computing, networks, and optimization theory.

Kaitai Liang [M'15] (k.liang@surrey.ac.uk) is currently an assistant professor in the Department of Computer Science, University of Surrey, United Kingdom. He received his Ph.D. degree from the Department of Computer Science, City University of Hong Kong, in 2014. His research interests are applied cryptography and information security; in particular, data encryption, blockchain security, post-quantum crypto, privacy enhancing technology, and security in cloud computing.

Xiaokang Zhou [M'12] (zhou@biwako.shiga-u.ac.jp) received his Ph.D. degree in human sciences from Waseda University, Japan, in 2014. He has been engaged in interdisciplinary research work in the fields of computer science and engineering, information systems, and social and human informatics. His recent research interests include ubiquitous and social computing, big data mining and analytics, behavior and cognitive informatics, machine learning, human-computer interaction, cyber intelligence, and cyber-enabled applications.