A Novel Identity-based Authentication Scheme for IoV Security

Changguang Wang, Zimeng Dai, Dongmei Zhao, and Fangwei Wang
(Corresponding author: Fangwei Wang)

Key Lab of Network and Information Security of Hebei Province
No.20, South ErHuan Road, YuHua District, Shijiazhuang 050024, China
College of Computer and Cyber Security, Hebei Normal University
No.20, South ErHuan Road, YuHua District, Shijiazhuang 050024, China
(E-mail: fw_wang@hebtu.edu.cn)
(Received Feb. 10, 2019; Revised and Accepted Aug. 3, 2019; First Online Sept. 8, 2019)

Abstract

In order to enhance the security of the IoV (Internet of Vehicles), a novel bi-directional authentication scheme is presented in this paper. By use of the elliptic curve encryption algorithm and the bilinear pair mapping theory, this scheme is designed to store the main system information in the RSU (Road Side Unit). During the process of communication, the shared key, identity ID, and handshake principle are used to perform mutual security authentication between the RSU and OBU (On Board Unit), thus ensuring the legitimacy of the communication nodes. Simulation experiments show that the computational complexity is reduced by about 10%, the efficiency and security of the scheme are improved compared with the existing schemes while meeting the security requirements.

Keywords: Authentication; Certificate Authority; On-Board Unit; Road Side Unit; Security

1 Introduction

The Internet of Vehicle (IoV) is an application of the IoT in road traffic and is also an important part of the Intelligent Transport System (ITS). Through advanced information and communication technology [7, 9, 22], such as GPS, sensing technology, network technology, and image identification technology, it can inform and help drivers to avoid accidents and even take control measures in case of emergency.

Consisting of interconnected entities on the road, IoV is created spontaneously and used to exchange data, perceive the traffic conditions, monitor the running state of the car, improve road traffic effectively and provide comfort for drivers and passengers. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) are two types of communication between entities on the road. In order to achieve the above functions, when vehicles pass through V2V or V2I, they will communicate and exchange information with their neighbor nodes. They send information automatically at set intervals to find and judge their neighbors and share the state information (position, speed, acceleration and direction) so that dangerous accidents can be avoided. On the other hand, emergency information can be transmitted to inform all nearby neighbors in the event of an emergency notice.

There are several available schemes of authentication, such as the authentication scheme based on an anonymous certificate, the authentication scheme based on a group signature, and the authentication scheme based on an RSU, and so on [4, 11].

The authentication scheme based on the anonymous certificates was proposed by Raya and Hubaux in 2007 [20]. The main idea is that vehicles need a large number of anonymous certificates, which are issued by CA (Certificate Authority) and stored in the OBUs of vehicles. When a vehicle needs communication, it will randomly select an anonymous certificate to sign the message which needs to be broadcasted and discard the certificate after signing, to ensure the security and privacy of the message and then hide the identity information of the vehicle. Accordingly, it can make the communication process untraceable. Besides, in order to track the vehicle in the event of an accident, CA will keep the correspondence between the real identity information and the anonymous certificate of the vehicle during registration, so that it can achieve the traceability of the malicious behaviors. Although this kind of scheme can ensure the anonymity of the message, there are still some deficiencies, among which the cancellation process is the largest weakness. When a vehicle is revoked, the cancellation information needs to be broadcasted across the network. A Certificate Revocation List (CRL) will load a lot of certificates, thus reducing the efficiency of message authentication. Besides, this kind of scheme makes a high request for the

OBU's storage capacity.

The authentication scheme based on a group signature was first proposed by Chaum and Van Heyst in 1991. In 2001, Dan Boneh proposed a signature scheme based on the elliptic curve and the ultra-short of the elliptic curve, whose signature length was half of the DSA. In 2007, Lin *et al.* proposed a GSIS scheme [13], which combined the group signature and the identity authentication technology. In 2010 Wasef *et al.* proposed a group signature scheme [26], which supported the vehicle batch validation for the IoV security. In 2011 Chim *et al.* proposed a group signature authentication scheme based on software [5], which used Bloom filter and binary search technology. In 2013, Zhu also proposed a group signature authentication scheme [31] which used hash value for CRL verification. This kind of scheme reduces the storage requirements on the OBU, but introduces the role of the group administrator which can be fatal to the entire IoV when being attacked. Moreover, it is difficult to balance the network scale. If the number of vehicle nodes in the group is large, the growth of CRL will be rapid, leading to the decline of node authentication efficiency. If there are few vehicle nodes in the group, for example, only one vehicle enters the group area, it can easily attack the network through the group identity information.

In IoV, RSUs are fixed units with large capacity and high transmission rate and are generally deployed at crossroads. Lu *et al.* proposed an ECPP protocol [15], which was characterized by generating a dynamic short-time anonymous key between the OBU and the RSU. The LPA protocol [28] proposed by Xue *et al.* introduced the concept of RSU neighbor set. The characteristics of the scheme are using RSU/OBU for online authentication and providing the certificate updates for OBU by RSU. This scheme can quickly generate anonymous keys, fast perform anonymous authentication and track privacy between the OBU and RSU while minimizing the storage for the anonymous key. Therefore, it can reduce the overhead and the complexity of the certificate management, and also provide good security and high efficiency for vehicle communication. In the RSU-based scheme, the amount of computation and the storage of OBU are far less than that of other schemes, but the signature and verification signature are largely dependent on RSU. Accordingly, V2V communication is not supported and all the communications are dependent on RSUs.

Lee *et al.* proposed an improved Identity-Oriented batch authentication scheme [10], but it could not resist a replay attack and could not satisfy traceability. Bayat *et al.* put forward another improved scheme [2] to improve the safety performance, but the scheme is designed only based on bilinear pairs, which is inefficient and cannot meet the time performance requirements of vehicle networking.

At present, the convergent signature authentication algorithm and the certificate free cryptosystem [8, 27] have been studied, but they are not suitable for IoV communication for the high computational cost and not able to resist some attacks such as identity forgery.

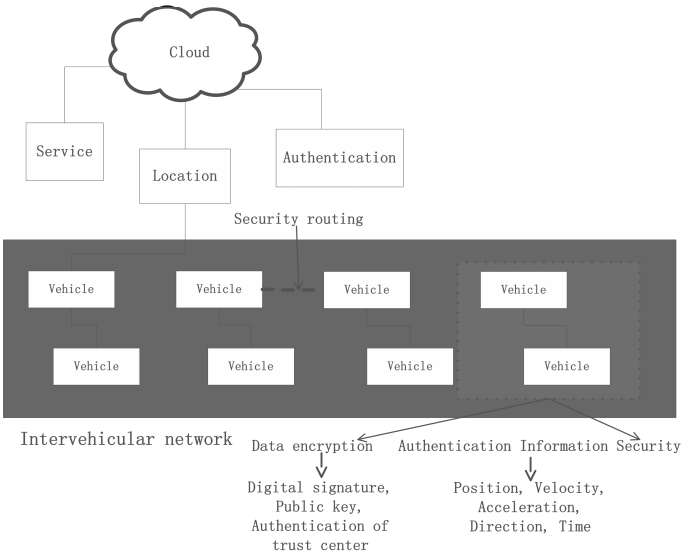


Figure 1: Security architecture of IoV

In this paper, we propose a novel identity-based bi-directional authentication scheme between OBU and RSU for IoV security based on considering the advantages and disadvantages of the existing schemes. Our scheme is designed by combining elliptic curve encryption with bilinear mapping theory, and can effectively make use of the characteristics of RSU to make the information transmission process more direct, fast and secure.

2 The Security Authentication Model

2.1 Network Model

The IoV security problems increase with the continuous development of its various applications. And the inherent characteristics of it, such as short distance, fast topology change, and openness, make the security threats even worst. The security architecture of it is shown in Figure 1.

Security requirements of the IoV mainly include non-forgery, privacy protection, traceability, revocability [14, 16, 30]. More and more secure authentication and privacy protection schemes are proposed to make the IoV nodes able to communicate with each other securely. In IoV, authentication is the core security requirement, which provides the integrity of information and avoids the manipulation of the exchanged information [25]. Fundamentally, all applications in IoV need to be authenticated [6, 19].

2.2 Identity Authentication Algorithm

Node identity authentication plays an important role in IoV researches. The most popular identity-based authentication algorithm is shown as follows [3]:

Algorithm 1 Identity-based authentication algorithm

1: **if** A is the identity **then**
2: Check whether VerA (A) is "valid"
3: Store A and its digest
4: **else if** A is the digest **then**
5: Verify whether A has been stored and whether it is valid
6: **end if**
7: Verify whether A exists in the RCL

2.3 Identity Authentication Model

In our scheme, there are mainly three entity parts which are CA, RSU, and OBU, respectively.

1) CA: The trust center mainly generates system parameters for the scheme and announce them to the public.

2) RSU: The roadside unit, the core part of the scheme, is used to store the main system information.

3) OBU: The onboard unit enables the vehicles to communicate with RSU or other vehicles.

Vehicle nodes can apply to CA for vehicle-related information when registering in the vehicle management office. The specific message construction is shown in Table 1.

Table 1: Message construction

Real ID of OBU
Private key of OBU
Certificate of OBU
Signature of OBU
Timestamp

Our scheme is designed based on the elliptic curve cryptography algorithm [12, 24, 29] and the bilinear pair mapping theory [23]. Here the hash function [18] is introduced to reduce the computational complexity. The scheme stores the main parameters of the system in the RSU instead of the OBU. When the vehicle arrives in the area covered by RSU, RSU and OBU need to perform mutual authentication. RSU judges whether to send the shared key for the OBU. OBU judges whether RSU is legal or not. If RSU is legal, OBU joins in the group. The main processes of the scheme include system initialization, RSU registration, OBU generating pseudonym identity, RSU and OBU mutual authentication, the RSU generating a temporary key, the OBU signing and transmitting the message, and revoking the identity. The specific model description is shown in Figure 2.

3 Scheme Flow

This paper proposes an identity-based mutual authentication scheme for IoV security, the specific process is shown in Figure 3.

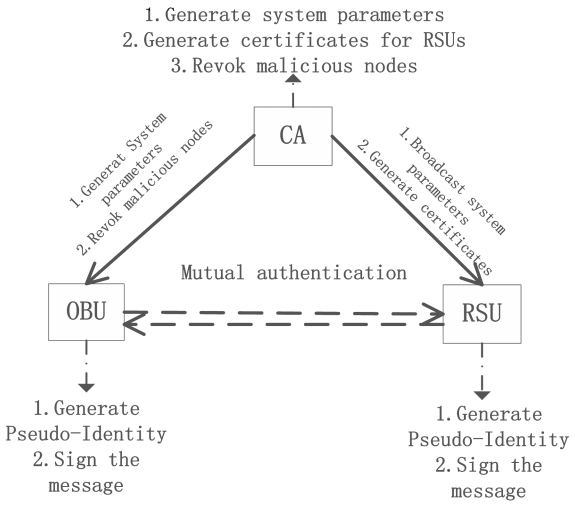


Figure 2: Schematic model

3.1 System Initialization

CA establishes system parameters for the scheme, which mainly includes the following aspects:

1) Define the finite field Z_q^* ={*0,1,2,3,. . . ,q-1*}, select the large prime number q, and select the elliptic curve $y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0 (\bmod q)$; define the cyclic additive group G_1 and the cyclic multiplicative group G_2. G_1 and G_2 have the same order q (q is a large prime number in the finite field), where $\hat{e} : G_1 \times G_2 \to G_2$ is the bilinear pairing principle. According to this principle, *CA* generates system parameters *(G_1, G_2,e,P,q)*, where P is the generator of the elliptic curve.

2) Define hash functions: $H1 : \{0,1\}^* \to G_1$, $H2 : \{0,1\}^* \times G_2 \to Z_q^*$.

3) In the finite field, *CA* selects a random number s as the system private key and then calculates $p = s \times P$ as the system public key.

4) *CA* selects the encryption and decryption functions *Ex(.)* and *Dx(.)* according to the elliptic curve encryption algorithm.

5) *CA* announces the parameters {G_1, G_2, q, P, s, p, $\hat{e}$, *H1(.), H2(.), Ex(.), Dx(.)*} to public, and stores them in RSU and OBU, respectively.

3.2 RSU Registration

1) *CA* selects a random number S_{RSU_j} in the finite field as the private key for each RSU and calculates $P_{RSU_j} = S_{RSU_j} \times P$ as the public key of RSU_j.

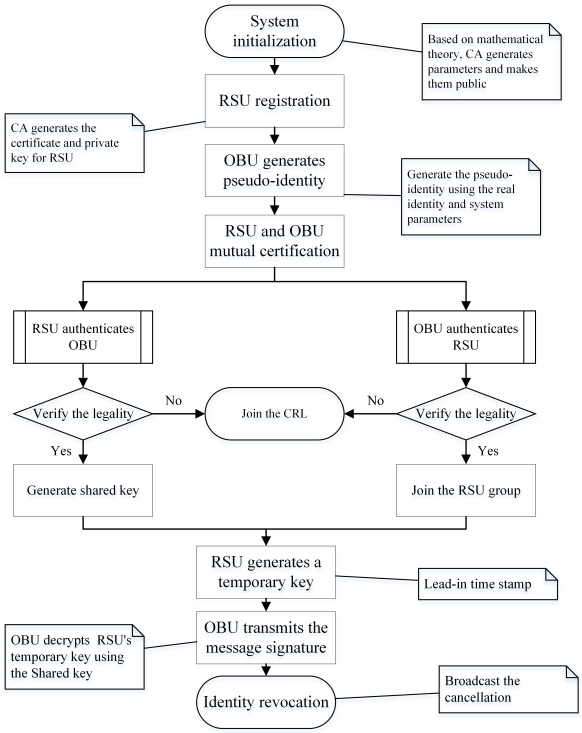


Figure 3: Flow chart of the scheme

2) *CA* uses the Schnorr scheme [17] to sign for each RSU. In the process of signature, ID_{RSU_j}, the identity of RSU_j, is used to select a random number k and a large prime number Q, where

$$\begin{aligned} m &= P^k \bmod Q, \\ e &= h(ID_{RSU_j} \| m), \\ d &= S_{RSU_j} e + k \bmod q. \end{aligned}$$

$Sign_{RSU_j}$ is *(d,e)*, and the generated certificate is $Cert_{RSU_j} = (P_{RSU_j}, Sign_{RSU_j})$

3) The generated certificate and private key are sent to each RSU through the security channel and stored in the RSU.

The process diagram is shown in Figure 4.

3.3 OBU Generates Pseudonym Identity

To ensure the traceability of vehicle nodes, sign the nodes based on OBU, and generate certificates $Cert_{OBU_i}$. The signature method is similar to RSU.

Here, each OBU uses real identity and public parameters to generate a pseudonym identity, thus can securely authenticate the OBU. The identity generation process is as follows:

$\mathbf{OBU}_i$ selects a random parameter r from the finite field

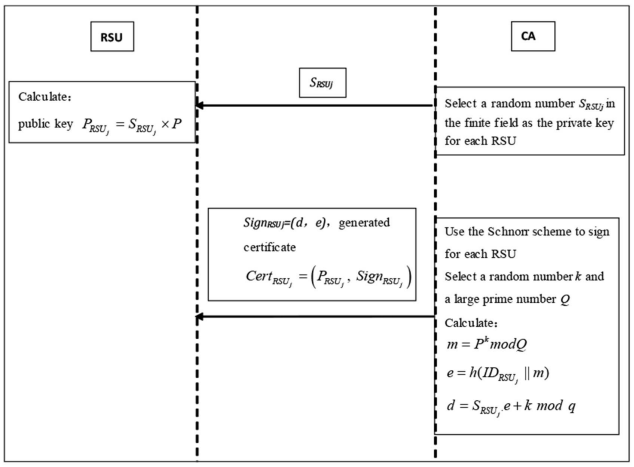


Figure 4: RSU registration process diagram

and then calculates

$$\begin{aligned} ID_i^{'} &= rP, \\ ID_i^{''} &= ID_i^R \oplus H2(rp), \\ ID_i &= \langle ID_i^{'}, ID_i^{''} \rangle. \end{aligned} \quad (1)$$

$\mathbf{ID}_i^R$ is the real ID of OBU_i, and ID_i is the pseudonym ID of OBU_i.

3.4 RSU and OBU Authenticate Mutually

In order to make it legal for the nodes of the communication process, each RSU and OBU perform mutual authentication to prevent malicious nodes from faking identity for attacks, thus guaranteeing the security of the system to the utmost extent.

1) RSU authenticates OBU
Before sending a message, OBU_i sends the pseudo-identity ID obtained in Step 3.3 to RSU_j through the secure channel, and RSU_j calculates the real identity ID of OBU_i through the public key p of the system.

$$ID_i^R = ID_i^{''} \oplus H2(sID_i^{'}).$$

After obtaining the real identity ID, RSU_j checks its own CRL to confirm whether OBU_i is legal, then selects a random integer n to calculate

$$S_{share} = H2((nP)_{S_{share}}).$$

It acts as a shared key between OBU and RSU, then it is sent to OBU_i.

2) OBU and RSU authenticate each other
OBU_i randomly selects *t1* from the finite field and then sends *t1* to RSU_j. RSU_j randomly selects *d, t2* from the finite field to calculate $N1 = Sign_{RSU_j} \times$

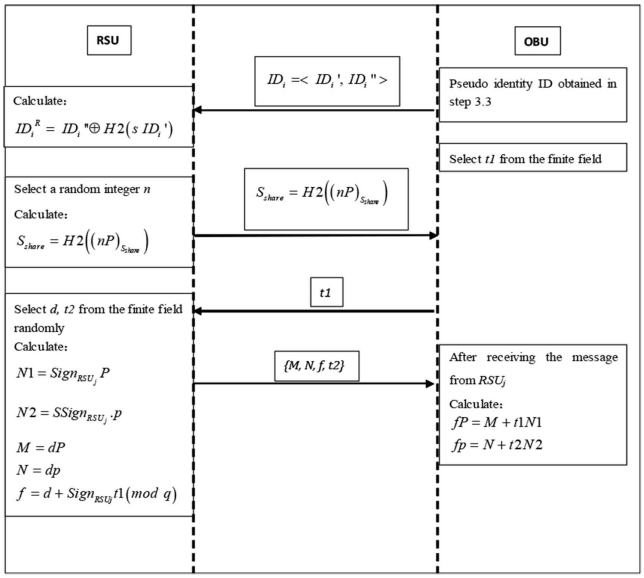


Figure 5: RSU and OBU authenticate mutually process diagram

$P, N2 = Sign_{RSU_j} \times p$ announces $N1$ and $N2$, calculates

$$\begin{aligned} M &= dP,\ N = dp \\ f &= d + Sign_{RSU_j} t1 (\text{mod } q) \end{aligned}$$

and then send $\{M, N, f, t2\}$ to OBU_i.

After receiving the message from RSU_j, OBU_i performs the following calculations:

$$fP = M + t1N1,\ fp = N + t2N2.$$

If the above equation is true, RSU_j is authenticated by OBU_i, and OBU_i will join the group of RSU_j to prepare for subsequent communication.

After RSU_j and OBU_i mutual authentication are completed successfully, OBU_i decrypts the shared key. The process diagram is shown in Figure 5.

3.5 RSU Generates a Temporary Key

RSU_j uses its primary private key to generate the temporary private key at the timestamp T_s, computes $S_{RSU_j}^{T_s} = H2(S_{RSU_j} \| T_s)$, generates the corresponding public key $P_{RSU_j}^{T_s} = S_{RSU_j}^{T_s} P$, and then broadcasts the public key. According to the elliptic curve encryption algorithm $E_{S_{share}}(S_{RSU_j}^{T_s}, Cert_{RSU_j}^{T_s})$, the private key is encrypted and the $\{nID_i^{'}, E_{S_{share}}(S_{RSU_j}^{T_s}, Cert_{RSU_j}^{T_s})\}$ is sent to OBU_i.

3.6 OBU Signs and Transmits Messages

Considering the time validity problem, the timestamp T_s is introduced, at which the temporary key of RSU_j is generated. OBU_i uses the temporary key of RSU_j to generate the pseudo identity and its corresponding key at the timestamp, and then uses the generated identity and key to sign the message for transmission.

1) OBU_i decrypts the shared key S_{share}
After receiving the message from RSU_j, OBU_i calculates the $S_{share} = H2((nID_i^{'} r^{-1})_{S_{share}})$ to get the shared key.

2) OBU_i decrypts the temporary key of RSU_j
After OBU_i obtains the shared key, it uses $D_{S_{share}}(S_{RSU_j}^{T_s}, Cert_{RSU_j}^{T_s})$ to decrypt and obtain the temporary private key $S_{RSU_j}^{T_s}$ of RSU_j.

3) OBU_i calculates the temporary pseudo-identity
OBU_i selects a random integer g from the finite field and calculates

$$\begin{aligned} ID_{T_s}^{'} &= gP, \\ ID_{T_s}^{''} &= ID_i^R \oplus H2(gP_{RSU_j}^{T_s}), \\ ID_i^{T_s} &= \langle ID_{T_s}^{'}, ID_{T_s}^{''} \rangle, \end{aligned} \quad (2)$$

where $ID_i^{T_s}$ is the temporary pseudo identity.

4) Calculate the temporary private key of OBU_i
The temporary private key of OBU_i is calculated as follows:

$$\begin{aligned} S_{OBU_i}^{T_s} &= \langle S_{OBU_i^{'}}^{T_s}, S_{OBU_i^{''}}^{T_s} \rangle \\ S_{OBU_i^{'}}^{T_s} &= S_{RSU_j}^{T_s} ID_{T_s}^{'} \\ S_{OBU_i^{''}}^{T_s} &= S_{RSU_j}^{T_s} H1(ID_{T_s}^{'} \| ID_{T_s}^{''} \| T_s). \end{aligned} \quad (3)$$

5) Sign the message M:

$$C = S_{OBU_i^{'}}^{T_s} + H2(M) S_{OBU_i^{''}}^{T_s}. \quad (4)$$

$(ID_{T_s}^{'}, C, M, ID_i^{T_s})$ will be sent to the recipient. The process diagram is shown in Figure 6.

3.7 Identity Revocation

According to the previous, the tracking and revocation of the malicious node can be performed by the information in the trust center and RSU_j. The trust center can judge the real identity of the malicious node by sending the master key in the RSU_j message, as follows:

$$ID_{T_s}^{''} \oplus H1(S_{RSU_j}^{T_s} ID_{T_s}^{'}) = ID_i^R \quad (5)$$

The trust center adds ID_i^R to the CRL and then broadcasts the CRL among the RSUs, thus the malicious node can never be authenticated or communicate with other nodes.

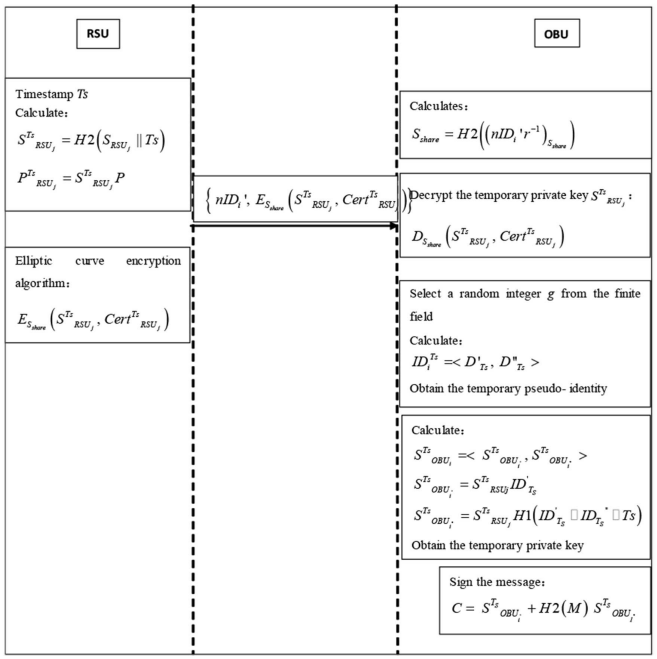


Figure 6: Sign and transmit messages process diagram

4 Performance Analysis

In this section, we will analyze the security of the scheme by means of formal analysis and simulation analysis whose simulation software is OMNET++.

4.1 Security Analysis

First of all, we analyze how the scheme meets the security requirements of IoV.

Non-forgery:

1) According to Equation (4), if we want to generate a valid signature, it is necessary for us to know the key S^{Ts}_{OBUi} which is generated by the temporary private key of the legal node RSU_j at timestamp T_s. This temporary key is encrypted with the Shared key and sent to the appropriate OBU along with the certificate. If we want to get S^{Ts}_{OBUi}, we need to know the shared secret S_{share} which is calculated by the random integer n. According to the mathematical difficult problems ECDLP, it is very difficult to calculate n. Because OBU and RSU have authenticated each other mutually before sending the message, the reliability between the communication nodes is high and the attacker cannot forge a signature.
2) If P, nID_i', rP are intercepted, according to Equation (1), the attacker needs to know r to calculate the pseudo-identity of OBU, so it can pass the RSU authentication, otherwise, it will be added to the revocation list. Considering the difficulty of ECDLP, if the user is malicious, the timestamp is invalid, which guarantees the unforgeability of the message.

Privacy protection:

1) According to the elliptic curve encryption algorithm and bilinear mapping theory, there are three basic difficult problems (ECDLP, BCDH, BDDH) that can guarantee the irreversibility of group operations, which makes it impossible for attackers to obtain the relevant certificate and key information through reverse engineering. When an OBU wants to get the temporary secret key of an RSU and join its communication group, it should use the hash functions to generate a temporary pseudonym identity ID according to the identity information and parameters of the trust center. Therefore, it can prevent the attacker from tracking the OBU as it moves between different RSUs.
2) RSU and OBU use the temporary keys in communication, while the generation of temporary keys uses the shared key generated in Section 3.4. According to Equations (2) and (3), the generation of temporary pseudo-identity uses the temporary keys S^{Ts}_{OBUi}, random integer g, and real identity ID_i^R . Moreover, as shown in Equations (3) and (4), the signature of a message uses different keys, and no node except the trust center and RSU can establish a relation between OBU_i*'s* pseudo-ID and the signature. Due to the mathematical difficult problems, the group operation is not reversible, so the privacy protection of the scheme is guaranteed.

Then we prove that our scheme satisfies security notions in the random oracle model.
Setting both sides of the game as attackers and challengers, the attacker is algorithm A running in polynomial time, the challenger is algorithm B, giving B a key exchange protocol input *(P, nP, bP, H)*, algorithm B uses A to solve the key agreement problem. The main steps are as follows:

System initialization: After selecting input *(P, nP, bP, H)*, algorithm B sends it to algorithm A.

Selection process: Algorithms A select ID_0^R and ID_1^R to Algorithms B.

Challenging process: Algorithms B randomly sets up a S_{share}, and then calculates the pseudo-identity of OBU:

$$\begin{aligned} ID_i^{'} &= nP, \\ ID_i^{''} &= ID_i^R \oplus H2(nbP), \\ ID_i &= \langle ID_i^{'}, ID_i^{''} \rangle. \end{aligned}$$

Guessing inquiry: A sends a guess about S_{share} to B. If the guess is right, then algorithm B solves the key agreement problem.

If $H = nbP$it can be calculated:

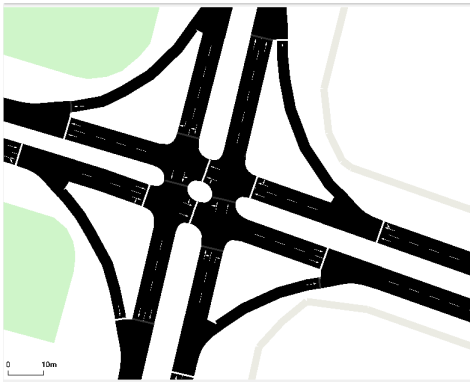
$$ID_x^{''} = ID_x^R \oplus H2(nbP) = ID_x^R \oplus H2(bID_x^{'}).$$

The probability of A guesses S_{share} is $1/2+\varepsilon$, then the probability of B's success is $1/2+\varepsilon$. Because H is randomly selected, ID_i^R it cannot be obtained, thus the probability of B solving the key agreement problem is $(1/2+\ \varepsilon\ +1/2)*1/2$, because ε it can be ignored, B can solve the problem. This is contrary to the assumption of key agreement difficulty and elliptic curve difficulty, so the scheme satisfies the privacy protection characteristics.

Traceability: Since all vehicles have been registered in the trust center and CA has the real identity of each vehicle, once a vehicle is attacked, the trust center can obtain the real identity information of the malicious node according to Equation (5), which ensures the traceability of the scheme.

Revocability: According to Section 3.7, when a vehicle is attacked and becomes malicious, the trust center can obtain its true identity and add it to the revocation list. When the malicious node initiates a communication again, RSUs will find that it is in the CRL and then refuse its communication request.

(a) Real view of the intersection



(b) Intersection Simulation

Figure 7: Map

4.2 Simulation Results

Our scheme is simulated by the use of Veins framework [21] which adopts SUMO as the transportation network platform and OMNET++ as the network simulation platform, respectively. Both platforms are based on C++. An RSU consists of three modules: appl, nic, and mobility. The nic module is based on the IEEE 802.11p protocol.

Due to the characteristics of large traffic flow and complex vehicle conditions, it is more meaningful for us to study the IoV authentication scheme at the crossroads. Therefore, we select a certain crossroad in Shijiazhuang urban area as the location of the simulation experiment. Figure 7(a) is a real scene map, and Figure 7(b) is a screenshot of the experimental environment. Taking this as an example, we analyze the delay, packet loss rate and signature efficiency of the scheme.

In this scheme, ECC is chosen as the main body of the cryptosystem. The security of ECC is based on the difficult problem of determining s with given sP and P, that is, the elliptic curve logarithm problem. The ECC key in the existing cryptosystem is short, the computation is small, the efficiency is high and the reliability is good.

1) Average delay: Because of the particularity of the IoV, messages are required to be transmitted as fast as possible. Thus, the time delay is an important index to measure the scheme performance. In our scheme, the time cost complexity is related to the time difference between message entering and quitting the Mac layer as follows:

$$D = \frac{\sum_{i=1} Sum(T_{out} - T_{in})}{Sum}$$

where Sum is the vehicle density, T_{out} and T_{in} are message entry and exit time, respectively. In this paper, the delay comparison is made between our scheme and ECPP scheme [15], Bayat's scheme [2] and Lee's scheme [10]. The experiment results are shown in Figure 8.

It can be seen from Figure 8 that the scheme performances have little difference when the vehicle density is small. With the increase of the vehicle density, the time delay of the authentication process increases accordingly and the performance differences of each scheme also increase gradually. In our scheme, on account of the higher efficiency of the adopted hash functions, the algorithm complexity is reduced. Therefore, the delay is lower and the performance is better compared with other schemes.

2) Packet loss rate: A too high packet loss rate will seriously affect data transmission. In this paper, the packet loss rate L of ECPP scheme [15], Bayat's

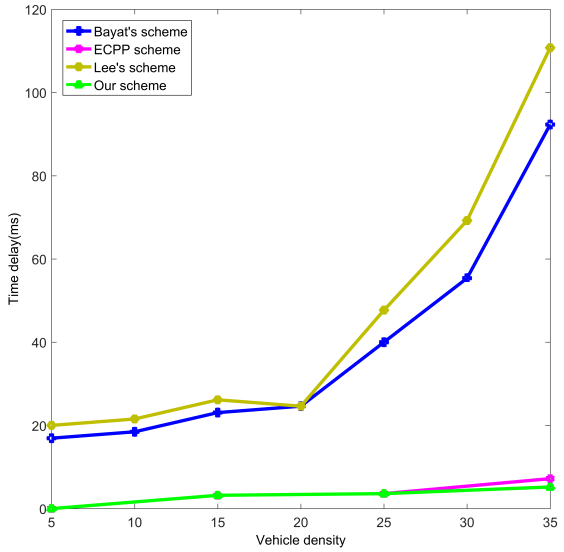


Figure 8: Relationship between delay and vehicle density

scheme [2] and Lee's scheme [10] are compared with that of our scheme. The calculation formula of the packet loss rate L is as follows:

$$L = \frac{\sum_{i=1}(M_r/M_l)}{Sum}$$

where Sum represents the density of communication vehicles, M_r is the total number of the received messages, and M_l is the total number of lost messages. Simulation results are shown in Figure 9.

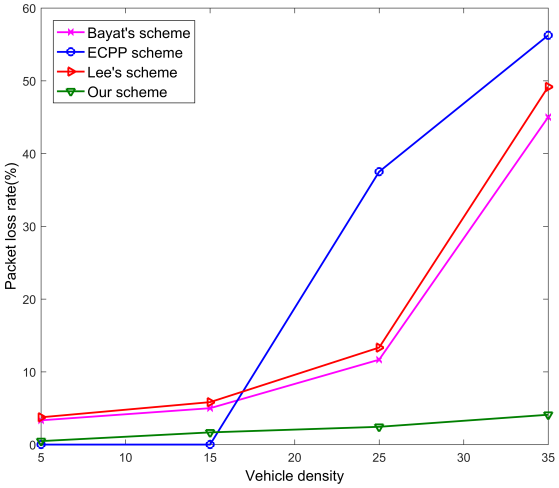
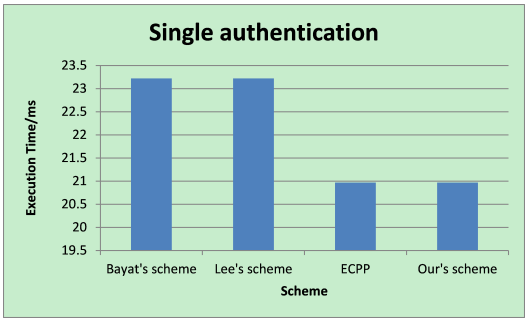


Figure 9: Packet loss rate

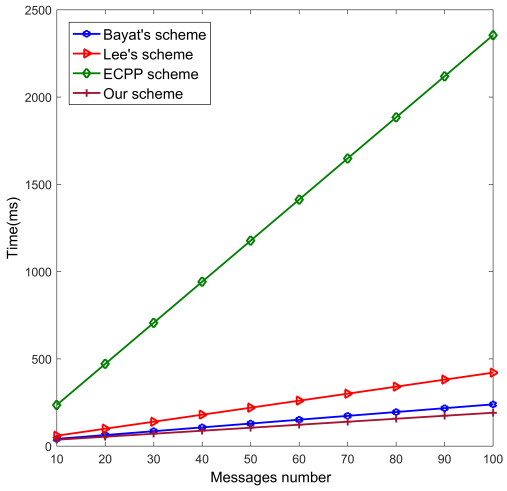
It can be seen from the figure that the performance of the scheme is similar when the vehicle density is small. With the increase of the vehicle density and the increase of communication load, ECPP and Bayat and Lee schemes have increased significantly. However, the packet loss rate of our scheme is still at a low level, mainly because the scheme reduces the computational complexity, reduces the delay and improves the efficiency of message processing.

3) Computational complexity: In this paper, the computational complexity of the scheme is compared with the computational complexity of the existing scheme. The computational formula is shown in Table 2.

The simulation results are shown in Figure 10. Figure 10(a) is the computational complexity of authenticating a single message and Figure 10(b) is the computational complexity of batch authentication.



(a) Single authentication



(b) Batch authentication

Figure 10: Authentication

The notations description in the formula is shown in Table 3 and the execution time is shown in Figure 11.

In this paper, the computational complexity of the scheme is compared with that of the existing scheme, as shown in Table 1, in which the description and execution time of each notation are shown in Table 2. According to the results, the complexity of this scheme is the same as ECPP, but lowers than Bayat's scheme and Lee's scheme; it is about 90% of these two schemes. With the increase of batch authentication messages, the scheme coefficient in this paper is 1.7177, which is less than that in other schemes, and the advantages are gradually obvious.

Table 2: Computational complexity comparison

Scheme	Single authentication	Batch authentication
Bayat's scheme	$3T_b+T_{bm}+T_H+T_h$	$3T_b+nT_{bsm}+3(n-1)T_{ba}+nT_H+nT_h$
Lee's scheme	$3T_b+T_{mul}+T_H$	$3T_b+nT_{bm}+3(n-1)T_{ba}+nT_H+nT_h$
ECPP scheme	$3T_b + T_{mul} + T_H$	$3nT_b+11nT_{mul}$
Our scheme	$3T_b+T_{mul}+T_H$	$3T_b+nT_{mul}+nT_H$

Table 3: Notation description

Notations	Description
T_b	Bilinear pairing operation
T_{bm}	Bilinear pair scalar multiplication
T_H	Map-To-Point hash function operation
T_h	One-way hash function operation
T_{bsm}	Bilinear pair small factor multiplication
T_{ba}	Additive operation
T_{mul}	Scalar Point Multiplication on Elliptic Curves

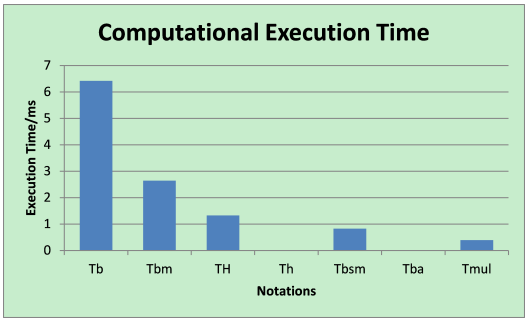


Figure 11: Computational execution time

The main reason is that the elliptic curve encryption and bilinear pairing used in our scheme has a shorter key and less work of computation. Besides, the Schnorr scheme is used to generate the certificate, and the main information of the system is stored in the RSU which has a large space. Therefore, our scheme is more efficient and stable than other schemes.

In this scheme, $Sign_{OBU_i}$ and $Sign_{RSU_j}$ are used to represent signatures. According to Schnoor signature algorithm, two parameters in group G_1 are used. In order to meet the security requirements of the system, the large prime q in the finite field is 170 bits and the element length in group G_1 is 171 bits, so the length of signature field is 171*2+170=512 bits, therefore the length of message is 173B, which is better than the existing scheme, which reduces communication overhead and improves authentication efficiency.

5 Conclusions

A novel identity-based authentication scheme is proposed in this paper. It is designed based on bilinear mapping theory, the elliptic curve encryption, and hash functions. At the beginning of communication, RSU and OBU authenticate each other through different algorithms to prevent malicious nodes from forging identities and to maximize the legality of the IoV nodes. Storing the main system information in RSU can be helpful to improve the efficiency of information exchange. Theoretical analysis proves that our scheme meets the requirements of non-forgery, privacy protection, traceability, and revocability. Simulation results show that our scheme has a smaller time delay, a lower packet loss rate, a lower computational complexity, and higher authentication efficiency compared with other schemes. Thus, it is more suitable for IoV applications [1].

In the following work, we will deeply study the impact of vehicle movement speed on message authentication, and further improve the privacy protection performance of the IOV.

Acknowledgments

The authors would like to thank the anonymous reviewers for their valuable suggestions given to improve the quality of the manuscript significantly. This work was supported by the National Natural Science Foundation of China under Grants No. 61572170 and No. 61672206, Program for Hundreds of Outstanding Innovative Talents in Higher Education Institutions of Hebei Province (III) under Grant No. SLRC2017042, Natural Science Foundation of Hebei Province of China under Grant No.F2018205162 and No.F2019205163, and Natural Sci-

ence Foundation of Hebei Normal University under Grant No.L072018Z10.

References

[1] T. Alam and B. Rababah, "Convergence of manet in communication among smart devices in IoT," *International Journal of Wireless and Microwave Technologies (IJWMT'19)*, vol. 9, no. 2, pp. 1–10, 2019.

[2] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless Networks*, vol. 21, no. 5, pp. 1733–1743, 2015.

[3] M. Boban and A. Festag, "Service-actuated multichannel operation for vehicular communications," *Computer Communications*, vol. 93, pp. 17–26, 2016.

[4] E. F. Cahyadi, C. Damarjati, M. S. Hwang, "Research on identity-based batch verification schemes for security and privacy in VANETs", *Journal of Electronic Science and Technology*, vol. 18, 2020.

[5] T. Chim, S. Yiu, L. Hui, Z. Jiang, and V. O. K. Li, "Specs: Secure and privacy enhancing communications schemes for VANETs," *Ad Hoc Networks*, vol. 9, no. 2, pp. 189–203, 2011.

[6] J. Cui, J. Zhang, H. Zhong, R. Shi, and Y. Xu, "An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks," *Information Sciences*, vol. 451-452, pp. 1–15, 2018.

[7] S. Hammad, R. A. Rehman, and B. S. Kim, "Services and security threats in sdn based VANETs: A survey," *Wireless Communications and Mobile Computing*, vol. 2018, no. 3, pp. 1–14, 2018.

[8] S. Horng, S. Tzeng, P. Huang, X. Wang, T. Li, and M. K. Khan, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Information Sciences*, vol. 317, pp. 48–66, 2015.

[9] M. Inam, Z. Li, A. Ali, and A. Zahoor, "A novel protocol for vehicle cluster formation and vehicle head selection in vehicular ad-hoc networks," *International Journal of Electronics and Information Engineering*, vol. 10, no. 2, pp. 103–119, 2019.

[10] C. Lee and Y. M. Lai, "Toward a secure batch verification with group testing for VANET," *Wireless Networks*, vol. 19, no. 6, pp. 1441–1449, 2013.

[11] C. T. Li, M. S. Hwang, Y. P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks", *Computer Communications*, vol. 31, no. 12, pp. 2803-2814, July 2008.

[12] J. Li, Y. Lin, R. Li, S. Zhou, and S. Wang, "Secure anonymous authentication scheme based on elliptic curve and zero-knowledge proof in VANET," *Journal on Communications*, vol. 34, no. 5, pp. 52–61, 2013.

[13] X. Lin, X. Sun, P. Ho, and X. S. Shen, "Gsis: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[14] P. Liu, B. Liu, Y. Sun, B. Zhao, and I. You, "Mitigating dos attacks against pseudonymous authentication through puzzle-based co-authentication in 5G-VANET," *IEEE Access*, vol. 6, no. 99, pp. 20795–20806, 2018.

[15] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *IEEE Computer and Communications Societies*, pp. 1229–1237, April 2008.

[16] S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Vehicular Communications*, vol. 9, pp. 19–30, 2017.

[17] H. Morita, J. C. N. Schuldt, T. Matsuda, G. Hanaoka, and T. Iwata, "On the security of schnorr signatures, dsa, and elgamal signatures against related-key attacks," *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, vol. 100, no. 1, pp. 73–90, 2017.

[18] W. Ng, X. Zhou, X. Tian, X. Wang, and D. Yeung, "Bagging-boosting- based semi-supervised multi-hashing with query- adaptive re-ranking," *Neurocomputing*, vol. 275, pp. 916–923, 2017.

[19] Q. Pei, B. Kang, L. Zhang, K. R. Choo, Y. Zhang, and Y. Sun, "Secure and privacy-preserving 3d vehicle positioning schemes for vehicular ad hoc network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, p. 271, 2018.

[20] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[21] C. Sommer, I. Dietrich, and F. Dressler, "Simulation of ad hoc routing protocols using omnet++," *Mobile Networks and Applications*, vol. 15, no. 6, pp. 786–801, 2010.

[22] C. Song, G. Tan, and N. Ding, "Rsu-coordinated multichannel mac protocol in vehicular ad hoc network (in chinese)," *Journal on Communications*, vol. 39, no. 11, pp. 10–22, 2018.

[23] C. Song, M. Zhang, W. Peng, Z. Jia, Z. Liu, and X. Yan, "Research on batch anonymous authentication scheme for VANET based on bilinear pairing," *Journal on Communications*, vol. 38, no. 11, pp. 35–43, 2017.

[24] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," *Journal of Communications and Networks*, vol. 11, no. 6, pp. 574–588, 2008.

[25] K. Verma, H. Hasbullah, and A. Kumar, "Prevention of dos attacks in VANET," *Wireless Personal Communications*, vol. 73, no. 1, pp. 95–126, 2013.

[26] A. Wasef and X. M. Shen, "Efficient group signature scheme supporting batch verification for securing vehicular networks," in *IEEE International Conference on Communications*, pp. 1–5, May 2010.

[27] H. Xiong, Z. Guan, Z. Chen, and F. Li, "An efficient certificateless aggregate signature with constant pair-

ing computations," *Information Sciences*, vol. 219, no. 10, pp. 225–235, 2013.

[28] X. Xue and J. Ding, "Lpa: A new location-based privacy-preserving authentication protocol in VANET," *Security and Communication Networks*, vol. 5, no. 1, pp. 69–78, 2012.

[29] L. Zhe and S. Hwajeong, "Iot-nums: Evaluating nums elliptic curve cryptography for iot platforms," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 720–729, 2019.

[30] H. Zhong, S. Han, and J. Cui, "Privacy-preserving authentication scheme with full aggregation in VANET," *Information Sciences*, vol. 476, pp. 211–221, 2019.

[31] X. Zhu, S. Jiang, L.Wang, L. Hui, and L. Zan, "Privacy-preserving authentication based on group signature for VANETs," in *IEEE Globecom Workshops*, pp. 4609–4614, Dec. 2013.

Biography

Changguang Wang is currently a professor in the College of Computer and Cyber Security of Hebei Normal University. His research interests include network and information security, wireless network security, IoV, *etc.*

Zimeng Dai is currently a Master degree student in the college of Computer and Cyber Security of Hebei Normal University. Her research interests include network and information security, sensor networks and IoV.

Dongmei Zhao is a professor at Hebei Normal University, Shijiazhuang, China. Her research interests include network and information security, network situation assessment, AI, *etc.*

Fangwei Wang is a professor at Hebei Normal University, Shijiazhuang, China. His research interests include network and information security, network worms,*etc.*