An Efficient Mutual Authentication Framework with Conditional Privacy Protection in VANET

Ying Wang, Jing Hu, Xiaohong Li(✉), and Zhiyong Feng

College of Intelligence and Computing, Tianjin Key Laboratory of Advanced Networking (TANK), Tianjin University, Tianjin 300350, China
{joycewang,mavis_huhu,xiaohongli,zyfeng}@tju.edu.cn

Abstract. Vehicular Ad Hoc Network (VANET) is a special application of traditional Mobile Ad Hoc Network (MANET) in traffic roads, which has attracted extensive attention due to its important role in intelligent traffic and road services. In order to ensure the safety of road traffic and protect the privacy of users, it is of vital importance to provide effective anonymous authentication in VANET. In this paper, we propose an efficient mutual authentication framework with conditional privacy protection (EMAPP), which can achieve the security authentication from vehicles to infrastructure and vehicles to vehicles. In the proposed framework, we are combined with pseudo ID and temporary pseudonym to protect the privacy of vehicles, and use the identity-based signature scheme to achieve authentication between vehicles and infrastructure. At the same time, with the assistance of the roadside unit (RSU), we utilize an online/offline signature scheme to achieve authentication between vehicles in the same RSU area and different RSU area. Our scheme has reusability, and we have conducted a performance evaluation. Without expensive and time-consuming operations such as bilinear pairing and mapping to point (MTP) functions, our framework can produce better performance and is appropriate for practical application. In addition, we also use the Internet Security Protocol and Application Automatic Authentication (AVISPA) tools to provide formal security analysis.

Keywords: VANET · Authentication · Conditional privacy protection · AVISPA · Formal proof

1 Introduction

In order to reduce the occurrence of traffic accidents and develop road entertainment services, people have focused on the development of intelligent transportation systems (ITS). Therefore, Vehicular ad hoc network (VANET), which is an important component of ITS, has developed rapidly in the past two decades [2]. In VANET, the vehicles equipped with On-Board Units (OBU) and infrastructure deployed along roads, called roadside units (RSU), form the nodes of

X. Wang et al. (Eds.): CollaborateCom 2019, LNICST 292, pp. 799–815, 2019.
https://doi.org/10.1007/978-3-030-30146-0_53

the network. And there are two types of communication in VANET: vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication, which are based on the Dedicated Short Range Communication (DSRC) [15] protocol.

The main purpose of VANET is to improve road safety by exchanging safety information. When safety information is transmitted in wireless channels, it can be easily eavesdropped, modified and deleted by malicious attackers. Therefore, in the face of these security attacks, the authentication of messages becomes a key security service for communication between vehicles and between vehicles and infrastructure in VANET. However, the traffic information exchanged in VANET may contain the drive's personal privacy, such as the driver's true identity, daily route, home address, etc. Some criminals may use the collected private information to hurt the driver. Therefore, the true identity of the vehicle should also be protected during the authentication process. At the same time, the illegal vehicle should also have the right to be revoked and exposed to their true identity.

At present, there are numerous research work related to the authentication problem in VANET, among which the widely adopted schemes are roughly divided into three categories: PKI-based authentication, ID-based authentication, and certificateless scheme. [8,10,12] are all PKI-based authentication schemes, but the common problem of these schemes is that additional communication is required to manage vehicle certificates and certificate revocation, which may impose heavy communication and computation costs on the network. [4,6,9,11,17] are all ID-based authentication frameworks. Among them, [9,17] adopt identity-based signature (IBS) and online/offline signature (IBOOS) schemes. By putting the pseudonym generated by the vehicle itself and the offline signature obtained by the vehicle from the RSU into a set, and broadcasting the set to the vehicles in the RSU area, the vehicles in the area can confirm the legal identities of other vehicles through the set, thus completing the authentication between the vehicles. However, as the number of certified vehicles increases, the set will also gradually increase, and the set needs to be updated after each successful verification of the vehicle, which will result in great communication overhead and high storage requirements for the vehicle. In addition, the framework is also vulnerable to impersonation attacks and Sybil attacks. Some vehicles may use pseudonyms and offline signatures of other vehicles in the set to communicate under the identities of other vehicles. Also, since the pseudonym of the vehicle is independently generated by itself, illegal vehicles may generate multiple pseudonyms, creating the illusion of multiple vehicles. In response to the problems in [9,17], we improved the scheme and proposed a different authentication process.

In this paper, we propose an efficient mutual authentication framework with conditional privacy protection (EMAPP). In the proposed framework, we adopt an identity-based signature scheme to ensure the authenticity and integrity of the message in the authentication process between the vehicle and the roadside unit, and through the identity-based online/offline signature scheme, with the assistance of the RSU, the identity authentication between vehicles is realized.

In addition, the vehicle can independently generate temporary pseudonyms to protect its privacy during the communication process. However, when the vehicle commits illegal activities, TA can track the vehicle according to the information source, restore its true identity and revoke the vehicle from the network, thus realizing conditional privacy protection. In addition, EMAPP is reusable, eliminates the need for expensive and time-consuming bilinear pairing and point mapping operations, and does not require the storage of key certificates and pseudonym sets, which greatly reduces the performance requirements of the vehicle.

Our framework is formally verified by using the formal tool AVISPA, and its performance is evaluated by quantitative calculation in terms of computational costs and communication overhead. The results show that the proposed EMAPP is secure and can achieve security objectives such as identity authentication, non-repudiation, identity privacy protection, traceability, etc. It can also resist Sybil attack, impersonation attack, modification attack, replay attack and repudiation attack. Our framework also achieves lower message latency and is more suitable for large-scale VANET.

The rest of this paper is organized as follows: in Sect. 2, some related work are reviewed. Section 3 describes some necessary preliminaries knowledge. Section 4 describes the proposed scheme. Section 5 provides a security analysis of the scheme. Section 6 provides a performance assessment of the proposed and other schemes. Section 7 concludes the paper.

2 Related Work

Currently, there are many jobs that can implement anonymous authentication in VANET, and these tasks can be divided into three categories: the public key infrastructure (PKI) based authentication, the identity (ID) based authentication and certificateless scheme.

– **the PKI based authentication:**

In 2004, Hubaux et al. [8] first proposed that PKI technology can be used to protect transmission messages in the vehicles. In 2007, Raya and Hubaux et al. [10] proposed an anonymous authentication scheme for VANET based on anonymous certificates. However, this scheme requires each vehicle to be preloaded with a large number of anonymous public/private key pairs and corresponding public key certificates, thus requiring huge storage space to store the keys. In 2008, Lu et al. [12] proposed an effective conditional privacy preservation (ECPP) scheme using temporary anonymous certificates to solve the problem of large storage space for vehicles. In short, PKI-based authentication schemes require additional communication to manage vehicle certificates and certificate revocation on and computational overhead.

– **the ID based authentication:**

Liu et al. [11] used the identity-based signature method of bilinear pairing to let the proxy vehicle verify the validity of the signatures on other vehicle messages

in batch, and RSU then checked the verification results of the proxy vehicle in batch. However, this scheme is vulnerable to sybil attacks, and if there is at least one invalid signature in the verification batch, the batch verification may fail. He et al. [6] proposed an identity-based signature scheme without bilinear pairing to reduce the computational complexity of bilinear pairing functions. Vehicles can also use self-generated pseudonyms to communicate anonymously with other vehicles and RSU. However, this scheme is also vulnerable to sybil attacks and global positioning system (GPS) spoofing attacks because no information is provided to prove the credibility of the location provided by the vehicles. Ons Chikhaoui et al. [4] proposed the use of temporary tickets to maintain the privacy of vehicles. This scheme obtains certificates and corresponding private keys from a trusted authority (TA) in the offline phase, and forms tickets by signing the certificates in the online phase to realize authentication between vehicles and RSU as well as between vehicles. However, this scheme needs to generate a set of certificates for vehicles in advance, and also needs to use a public key certificate to ensure that vehicles can safely obtain new certificates and private keys from TA before the current certificate set is used up, thus requiring higher storage requirements.

– **certificateless scheme:**

Horng and Tzeng et al. [7] proposed a provably secure CCPPA scheme based on certificateless cryptography. In this scheme, part of the private key of the user (vehicle and RSU) is generated by the Trusted Key Generator Center (KGC), while the complete private key is formed by the user selecting a secret value and combining part of the keys, so KGC cannot obtain the user's private key. In addition, Yang et al. [14] proposed a certificateless conditional privacy protection authentication scheme in 2019. The scheme does not use hash mapping to points and l batch message authentication.

3 Preliminaries

In this section, we will introduce the system model, security goals, and the signature schemes to be used in the authentication process, such as the signature scheme BNN-IBS between the vehicle and the RSU, and online/offline signature scheme without key escrow between vehicles.

3.1 System Model

As shown in Fig. 1, VANET typically consists of three parts: trusted third-party TA, roadside infrastructure RSU, and OBU-equipped vehicles.

– **TA** is a trusted authority in VANET. It has powerful computing and storage capabilities and is responsible for generating the primary initial parameters for RSUs and OBUs in the region. Each car must be registered with the TA before joining the network, so the TA can store the real information of the vehicle, and it is also the only party that has the right to reveal the user's

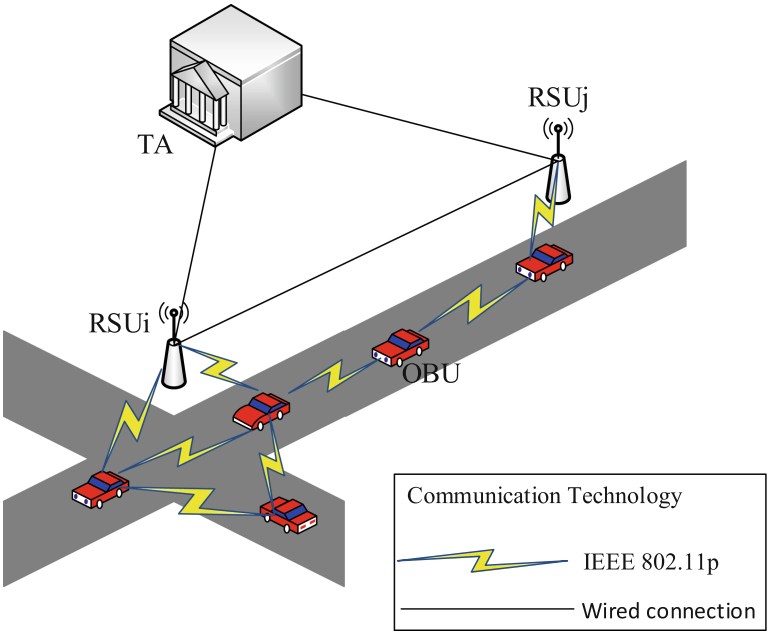

Fig. 1. System model.

identity. If there is malicious and false information in the road network, the TA can track and identify the information source to resolve the dispute. In addition, the TA is considered unable to compromise with its opponents and is fully trusted by all parties in the system.

- **RSU** is an infrastructure distributed on the roadside. It communicates securely with the TA via a wired link and communicates with the OBU via the DSRC protocol, so he is semi-trusted. RSU will obtain the revocation list from TA, assist TA in verifying the legality of the vehicle identity within its area, and give the vehicle verification certificate so that the vehicle can communicate with other verified legal vehicles. In addition, it can also provide services such as Web and TCP to OBU. Each RSU is equipped with a Tamper Proof Device (TPD) to increase the reliability of the VANET.
- **OBU** is the internal processing unit of the vehicle. It enables vehicles to wirelessly communicate with other vehicles and RSUs based on the DSRC protocol and uses TPD to store their sensitive information. When the vehicle is driving, it broadcasts information such as location, time, speed, vehicle path and traffic conditions to other vehicles and RSUs. If it receives false information or suffers some attacks during vehicle communication, it can report to TA through RSU.

3.2 Security Goals

In VANET, in order to protect the security of users' information, users must authenticate their identities anonymously. However, if some vehicles send out

fraudulent messages, there must be a trusted authority that can track and reveal the actual identities of the vehicles, which is also called conditional privacy protection. Besides, due to the high-speed changes of the VANET network topology and other characteristics, the efficiency and feasibility of the scheme must also be considered, so the safety objectives of the proposed scheme should focus on the following points:

- **Message authentication:** the receiver of the message should be able to verify the integrity of the message and the legitimacy of its source.
- **Identity privacy protection:** TA should be the only party that can disclose the true identity of the vehicle.
- **Identity revocation:** In order to protect the safety of other legitimate vehicles, misbehaving vehicles should be expelled from the network.
- **Non-repudiation:** The sender of the message should not deny having sent that message.
- **Defense against multiple attacks:** The scheme should be able to resist a variety of attacks, such as identity analysis attack, impersonation attack, Sybil attack, modification attack, replay attack and repudiation attack.

3.3 BNN-IBS Scheme

The BNN-IBS [13,16] scheme is based on elliptic curve cryptography, and it dose not use time-consuming and expensive bilinear pairing and mapping to point hash functions. It mainly includes the following four steps:

- **Setup:** TA generates system parameters, including master key sk and corresponding public key PK, and publishes the system parameters to the network, sk keeps the secret.
- **Extract:** TA calculates the private key rk of the RSU and the private key vk of the OBU based on the master key sk and the given ID.
- **Sign:** Given the ID, the corresponding private key and the message m, a signature $\sigma(m)$ is generated, and it is a triplet containing the public key.
- **Verify:** Given the signature $\sigma(m)$, the corresponding public key and the message m, after the relevant calculation, the signature is accepted if the answer is yes and rejected otherwise.

3.4 Online/Offline Signature Scheme Without Key Escrow

The identity-based cryptography (IBC) scheme has serious security issues due to key escrow, and the scheme [5] avoids key escrow problems by adopting the idea of Certificateless Cryptography (CLC). It mainly includes the following steps:

- **Setup:** TA generates system parameters and publishes them to the network.
- **Extract:** The RSU extracts the signature private key and public key according to the master key.

- **Off-sign:** A probabilistic algorithm that calculates an offline signature $\sigma_{off}(ID)$ by entering system parameters, the corresponding ID and a signature private key.
- **On-sign:** Given the message m and the offline signature $\sigma_{off}(ID)$, it outputs online signal $\sigma_{on}(\sigma_{off}(ID)\|m)$, and give the full signature.
- **Verify:** An auxiliary algorithm that outputs an acceptance or rejection after verification by inputting the message m, the ID, the public key and the full signature.

4 The Proposed Framework

Our framework can be described from four phases: the system initialization phase, the R2V authentication phase, the inner-V2V authentication phase and the cross-V2V authentication phase. The symbols used in our scheme are listed in Table 1. Table 2 describes the general operations of the framework.

Table 1. The used notations

Notations	Description
TA	The trusted authority
E/F_q	An elliptic curve E over a finite field F_q
q	The field size
p	A large prime number
P	A point of order p on the curve E
G	A cyclic group of order p under the point addition "+" generated by P
sk, PK	The private key and public key of TA
ID_i, ID_{vj}	The identity of RSU_i, the identity of OBU_j
GC_i	The geographical coordinates of RSU_i
rk	The private key of RSU
PID_i	The pseudo identity of the OBU_i
vk	The private key of OBU
rt, prt	The temporary private key and public key of RSU
$\sigma_{ri}(), \sigma_{vj}()$	The signature of RSU_i and the signature of OBU_j
T	The time stamp of R2V authentication
n	A random number
vt, pvt	The temporary private key and public key of OBU
t	The time stamp of V2V authentication
PS_i	The pseudonym of OBU_i
RID	The real identity of the OBU
TID	The signature ID of offline signature, $TID = PS\|\sigma^*(PS)$
$\sigma^*()$	The signature does not contain the public key
$\sigma_{off}, \sigma_{on}$	The offline and online signature
$qr, result$	The query request, the query result

4.1 System Initialization

1. TA establishes the network parameters through the BNN-IBS setup algorithm, and then publishes the parameters $\{E/Fq, G, P, q, p, PK, H_1, H_2\}$ to the network, sk as its master key, $PK = skP$ as its master public key, and keep sk secret.
2. TA sets the identity of the RSU as the connection between its geographic coordinates and the serial number of the RSU. The identity of RSU is $ID_i = GC_i \| SQN$. Then it calculates the private key rk of the RSU through the key extraction algorithm in the BNN-IBS scheme, and sends $< ID_r, R_s, rk >$ to the RSU through a secure channel, the RSU can verifies the validity of rk by verifying $R_s + cPK = rkP$. R_s is defined in [16].
3. TA calculates the private key vk of the OBU through the key extraction algorithm of the BNN-IBS, and calculates the pseudo identity PID_i of the OBU by using PK:
   - Choose at random $w \in Z_p^*$, and compute
   - $PID_1 = wP$
   - $PID_2 = ID_v \oplus H_1(wPK)$
   - $PID_i = < PID_1, PID_2 >$
4. TA sends $< PID_i, R_v, vk >$ to OBU safely, and OBU can verifies the validity of vk by verifying $R_v + cPK = vkP$.

Table 2. Operations of the proposed EMAPP

R2V authentication	
Step 1. $RSU_r \Rightarrow *:$	$< ID_r, T, prt, \sigma_{r1}(ID_r \| T \| prt), n_r >$
Step 2. $OBU_i \rightarrow RSU_r:$	$< PS_i, T, \sigma_v^*(PS_i), \sigma_{v1}(\sigma_v^*(PS_i) \| T), n_r >$
Step 3. $RSU_r \rightarrow OBU_i:$	$< PS_i, \sigma_{off}(TID), T, \sigma_{r2}(\sigma_{off}(TID) \| T), n_r >$
Inner V2V authentication	
Step 1. $OBU_i \rightarrow OBU_j:$	$< PS_i, \sigma_i(PS_i), t, \sigma_{on}(\sigma_{off}(TID_i) \| t), n_i >$
Step 2. $OBU_j \rightarrow OBU_i:$	$< PS_j, \sigma_j(PS_j), t, \sigma_{on}(\sigma_{off}(TID_j) \| t), n_i >$
Cross V2V authentication	
Step 1. $OBU_i \rightarrow OBU_j:$	$< PS_i, \sigma_i(PS_i), t, \sigma_{on}(\sigma_{off}(TID_i) \| t), n_i >$
Step 2. $OBU_j \rightarrow RSU_j:$	$< (PS_j, \sigma_j(PS_j), T, \sigma_{on}(\sigma_{off}(TID_j) \| T), n_j, qr) >$
Step 3. $RSU_j \rightarrow OBU_j:$	$< PS_j, \sigma_{off}(PS_j \| PS_i), T, result, \sigma_{rj}(result \| T), n_j >$
step 4. $OBU_j \rightarrow OBU_i:$	$< PS_j, PS_i, ID_j, \sigma_{on}(\sigma_{off} \| ID_j), t, \sigma_{vj}(PSj \| t), n_i >$

4.2 R2V Authentication

1. The RSU calculates the temporary key $rt = H_2(rk \| Tr_1)$ according to the private key rk, Tr_1 is the validity period, and the corresponding public key $prt = rtP$. Then RSU calculates σ_{r1} through BNN-IBS algorithm, and periodically broadcasts the messages $< ID_r, T, prt, \sigma_{r1}(ID_r \| T \| prt), n_r >$ within its range, T is the current time interval.

2. The OBU firstly calculates the temporary key $vt = H_2(vk\|Tr_2)$ according to the private key vk, Tr_2 is the validity period, and the corresponding public key $pvt = vtP$. Then, after receiving the message, the OBU performs the following steps:
   - OBU checks the freshness of T.
   - If T is fresh then the OBU verifies GC_r in ID_r through GPS.
   - If GC_r is correct, the OBU verifies σ_{r1} through the BNN-IBS algorithm.
   - If the verification passes, the OBU generates pseudonym

$$PS_i =< T_{start}\|Enc_{prt}(PID)\|ID_r\|T_{end} >$$

   and signature σ_{v1}, T_{start} is the time when the pseudonym is generated, and T_{end} is the validity period of the pseudonym. Then the OBU sends the RSU the message:

$$< PS_i, T, \sigma_v^*(PS_i), \sigma_{v1}(\sigma_v^*(PS_i)\|T), n_r >$$

   Note that according to the BNN-IBS scheme, the signature is a triple containing the public key, but in this case, $\sigma_v^*(PS_v)$ is a two-tuple that does not contain the public key.
3. Once the RSU receives the message sent by the OBU, it performs the following steps:
   - the RSU first checks whether the T is fresh.
   - If T is fresh, the RSU obtains the PID in the pseudonym and the real ID of the OBU according to the parameters in the TPD, $ID_v = PID_2 \oplus H_1(skPID_1)$, then the RSU checks whether the vehicle is in the control revocation list (CRL) according to the obtained ID_v.
   - If it is, the OBU is rejected. If not, the σ_{v1} is verified by the BNN-IBS verification algorithm.
   - If σ_{v1} passes the verification, the RSU stores the PS_v and sends the PS_v and the PID to the TA. Then TA obtains the real ID of the vehicle according to the PID, and searches the record according to the ID to check whether it has used the pseudonym before. If not, it stores the pseudonym and PID. If there is, it updates the pseudonym and checks whether the pseudonym used before is expired. If not, the pseudonym used before will be revoked from the network.
   - Next, RSU uses its own temporary private key rt, generates the offline signature $\sigma_{off}(TID)$ according to the signature scheme [5], where $TID = \sigma_v^*(PS_i)\|PS_i$ is the signature ID. Then the RSU send the message

$$< PS_i, \sigma_{off}(TID), T, \sigma_{r2}(\sigma_{off}(TID)\|T), n_r >$$

   to the OBU. If the signature σ_{r2} is valid, the OBU will store the $\sigma_{off}(TID)$.

4.3 Inner V2V Authentication

1. OBU_i generates online signature and sends a message to OBU_j, the message is:
$$< PS_i, \sigma_i(PS_i), t, \sigma_{on}(\sigma_{off}(TID_i)\|t), n_i >$$
Note that $\sigma_i(PS_i)$ is a triple containing the public key pvt.
2. After receiving the message, OBU_j performs the following steps:
   - OBU_j checks the ID_r in the pseudonym to confirm whether OBU_i is in the same area as itself.
   - If it is, it first verifies the $\sigma_i(PS_i)$, and then verifies the online/offline signature by using the public key prt.
   - If the verification passes, it will reply to the message:
$$< PS_j, \sigma_j(PS_j), t, \sigma_{on}(\sigma_{off}(TID_j)\|t), n_i >$$
OBU_i will verify the identity of OBU_j in the same way.

4.4 Cross V2V Authentication

1. OBU_i sends a message to OBU_j, the message is:
$$< PS_i, \sigma_i(PS_i), t, \sigma_{on}(\sigma_{off}(TID_i)\|t), n_i >$$
2. When OBU_i and OBU_j are not in the same area, OBU_j sends RSU_j the inquiry request message
$$< (PS_j, \sigma_j(PS_j), T, \sigma_{on}(\sigma_{off}(TID_j)\|T), n_j, qr) >$$
qr contains PS_i, $\sigma_i(PS_i)$, t and $\sigma_{on}(\sigma_{off}(TID_i)\|t)$.
3. RSU_j queries other RSUs to check the validity of the OBU_i, if the OBU_i is a legitimate vehicle, RSU_j will return the inquiry result and give the vehicle OBU_j a ticket that can prove itself. The RSU_j sends the message to the OBU, the message is:
$$< PS_j, \sigma_{off}(PS_j\|PS_i), T, result, \sigma_{rj}(result\|T), n_j >$$
$\sigma_{off}(PS_j\|PS_i)$ is generated by the RSU_i in where OBU_i is located.
4. If the OBU_i is legal, OBU_j will send the message
$$< PS_j, PS_i, ID_j, \sigma_{on}(\sigma_{off}(PS_j\|PS_i)\|ID_j), t, \sigma_{vj}(PSj\|t), n_i >$$
to OBU_i, OBU_i can verify that OBU_j is a legitimate vehicle after getting the signature $\sigma_{on}(\sigma_{off}(PS_j\|PS_i)\|ID_j)$.

5 Security Analysis

In this section, we use the Internet Security Protocol and Application Automated Authentication (AVISPA) formalize our work and analyze security requirements presented before.

5.1 Formal Security Validation

The formal tool AVISPA [1] describes the security protocols and checks their security properties using HLPSL language. It contains four back-ends, OFMC, CL-AtSe, SATMC and TA4SP. Because V2V communication depends on R2V communication, we formally verified V2V communication process with AVISPA.

Part of the code after the formalization of our framework is given in Fig. 2. It provides entities authentication and secrecy of the message. Figure 3 shows the verification results of the inner-V2V communication under the OFMC model and the CL-AtSe model, which shows that the communication process is SAFE. The results of the cross-V2V communication are illustrated in Fig. 4.

```
RCV(IDr.Ks.T.H1(IDr.Ks.T))=|>State':=2/\N1':=new()
      /\PS1':=IDr.{IDv}_Ks
      /\TID1':=H2(PS1'.inv(Ku))/\secret(IDv,id,{B,R})
      /\SND(PS1'.TID1'.H2(TID1'.T).N1'.T)
RCV(PS1'.H1(TID1'.PS1'.inv(Ks)).T.H1(H1(TID1'.PS1'.inv(Ks)).T).N1')
      =|>State':=3/\N2':=new()
      /\SND(PS1'.Ku.TID1'.T2.H2(H1(TID1'.PS1'.inv(Ks)).T2).N2')
      /\witness(B,C,c_b_tid,TID1')
```

Fig. 2. Partial code for formal verification.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/inner-V2V.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
```

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/inner-V2V.if

GOAL
  As Specified

BACKEND
  CL-AtSe
```

Fig. 3. Results of inner-V2V communication.

5.2 Message Authentication

All RSUs and OBUs will sign the outgoing message. When processing a secure message, the receiving vehicle must verify the validity of the online/offline signature in order to check the legitimacy of the latter.

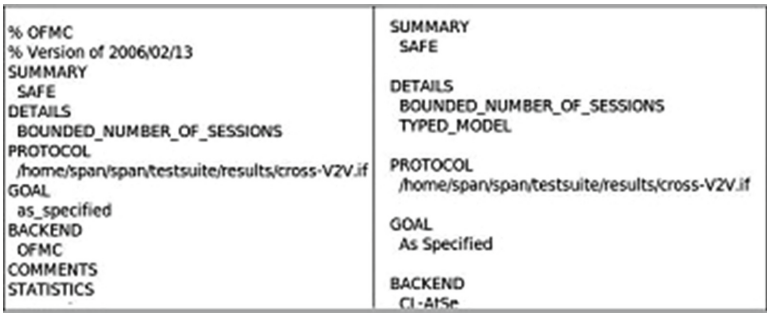

Fig. 4. Results of cross-V2V communication.

5.3 Identity Privacy Preservation

All vehicles use pseudonyms in the communication process. The ID of the vehicle in the pseudonym is a pseudo ID. The RSU can only know the real ID of the vehicle through the parameters in the TPD, but it cannot be saved. Only the TA knows and can save the real ID of the vehicle. When the RSU updates the key, or the pseudonym expires, the vehicle must re-authenticate to the network, so no attacker can obtain the true identity of the vehicle from the transmitted message.

5.4 Traceability

All vehicles use pseudonyms in the communication process. The ID of the vehicle in the pseudonym is a pseudo ID. The RSU can only know the real ID of the vehicle through the parameters in the TPD, but it cannot be saved. Only the TA knows and can save the real ID of the vehicle. When the RSU updates the key, or the pseudonym expires, the vehicle must re-authenticate to the network, so no attacker can obtain the true identity of the vehicle from the transmitted message.

5.5 Defense Against Several Types of Attacks

1. **Impersonation attack:** every vehicle in the network must get the online/offline signature of the RSU before communicating with other vehicles, and the identity of the vehicle must be verified again before verifying the online/offline signature, thus ensuring that the vehicle identity will not be being impersonated.
2. **Sybil attack:** a malicious vehicle may create the illusion of multiple vehicles by generating multiple pseudonyms. However, in our scheme, each vehicle must be certified by RSU and TA before communicating with other vehicles. The TA saves the vehicle's real ID, pseudo ID and currently used the pseudonym, which has a valid period. If the vehicle applies for a new

pseudonym before the expiration date of the pseudonym, the TA will revoke the old pseudonym from the network, thus ensuring that multiple pseudonyms will not coexist in the network at any time for each ID. Therefore our plan can prevent the Sybil attack.

3. **Replay attack:** each vehicle and RSU include a timestamp and a random number in each message, they send to detect the replay of the message.
4. **Modification attack and repudiation attack:** Our scheme adopt an identity-based signature scheme. And according to the above analysis, it can resist modification attacks and denial attacks.

6 Performance Evaluation

We compare the proposed EMAPP with ACPN [9] and MADAR [17] in terms of computational cost and communication overhead. Table 3 shows the time and size measurement for different operations, which is used to estimate the computational overhead and communication cost of the framework.

Table 3. Time and size measures of operations for evaluation.

Scheme	Operation	Time (ms)	Size of signature
BNN-IBS [3]	Sign	0.442	100B
	Verify	1.326	
Online/offline signature [5]	Sign/verify(online)	0.066	80B
	Offline	0	80B
ECDSA [17]	Sign	1.24	64B
	Verify	2.33	
IBOOS [9]	Sign/verify(online)	0.19	60B
	Offline	0	40B

6.1 Computation Cost

Due to the reusability of our framework, we can adopt a more efficient signature scheme to improve the performance of the proposed EMAPP. In order to better compare the proposed EMAPP with other schemes, in the experiment, we first used the same signature scheme as ACPN and MADAR to generate digital signatures for our framework. In Table 4, EMAPP-Y represents the computational overhead incurred when our scheme adopts ECDSA and IBOOS signature schemes, and EMAPP-N represents the computational overhead incurred when we adopt BNN-IBS scheme and online/offline signature scheme in Table 3.

As can be seen from the table, when the signature schemes are the same, our framework only has about $1 - 2\,ms$ more computational overhead than ACPN and MADAR, but our framework can resist impersonation attacks. The proposed

Table 4. Computation costs of OBU and RSU for different schemes (ms).

Phase	Subject	ACPN	MADAR	EMAPP-Y	EMAPP-N
R2V	OBU	5.900	6.600	7.140	3.536
	RSU	4.810	4.860	4.810	2.210
inner-V2V	Sender	0.190	0.380	2.710	1.458
	Receiver	0.190	0.380	2.710	1.458
cross-V2V	Sender	0.190	4.850	2.710	1.458
	Receiver	5.000	3.760	3.950	1.900
	RSU	3.570	2.860	6.280	3.226

EMAPP adds a process of verifying the pseudonym of the vehicle in the communication process, preventing other vehicles from posing as the identity of the vehicle when the offline signature and pseudonym are leaked. In addition, when our framework adopts BNN-IBS signature scheme and online/offline signature scheme, the computational overhead required is reduced by approximately half. Therefore, our framework has the possibility to further reduce the computational cost.

Besides, there are two kinds of V2V communication in EMAPP, which have different computation costs. In order to understand the influence of the proportion of vehicles participating in inner-V2V or cross-V2V communication on the overall computation costs, we use the same method as [9] to analyze the total cost of each communication process. In the procedure of vehicle-roadside communication, the computation delay T_{R2V} is calculated as:

$$T_{r2v} = 2T_{rsu\_sign} + 2T_{v\_verify} + 2T_{v\_sign} + T_{rsu\_verify} + T_{rsu\_offsign}$$

In the procedure of inner-V2V authentication, the computation delay T_{inner} is calculated as:

$$T_{inner} = T_{snd\_onsign} + T_{rcv\_onverify} + T_{rcv\_verify} + T_{rcv\_onsign} + T_{snd\_onverify} + T_{snd\_verify}$$

In the procedure of cross-V2V authentication, the computation delay T_{cross} is calculated as:

$$T_{cross} = T_{snd\_onsign} + T_{rcv\_onsign} + T_{query} + T_{snd\_verify} + T_{rcv\_sign} + T_{snd\_onverify}$$

where T_{query} is the process of communication between receiver and the RSU, and its calculation is as follows:

$$T_{query} = T_{rcv\_onsign} + 2T_{rsu\_onverify} + 2T_{rsu\_verify} + T_{rsu_offsign} + T_{rsu_sign} + T_{rcv_verify}$$

we can define γ as the proportion of vehicles participating in inner-regional communication. The value of γ can be calculated by $N_{inner}/(N_{inner} + N_{cross})$, and the ratio of vehicles who use cross-regional communication is $1-\gamma$. Therefore, the average computation delay of V2V authentication is calculated as:

$$T_{v2v} = \gamma \Delta T_{inner} + (1 - \gamma)\Delta T_{cross}$$

Figure 5 illustrates the effect of the proportion of inner-regional communication on the total calculation cost in different schemes. The results show that with the increase in the proportion of internal communication, the computation cost will be lower and lower, that is, the authentication efficiency will be higher and higher. We can also see that when the framework adopts a more efficient signature scheme, the efficiency of V2V communication is less affected by γ.

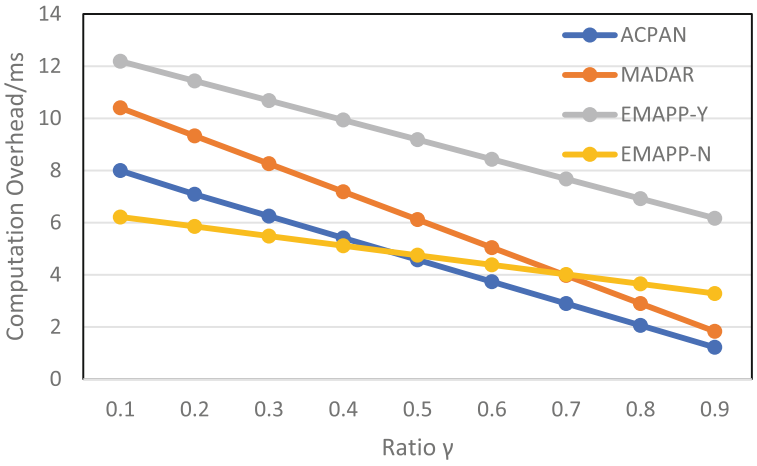

Fig. 5. Comparison on Computation Overhead (V2V).

6.2 Communication Cost

We estimate the communication cost by the length of the message. For the convenience of comparison, we use the length of some parameters in [17], such as the ID of RSU, the ID of OBU, the random number and timestamp, so we mainly consider the lengths of pseudonyms and signatures to compare the communication overhead. In our scheme, we select the same curve parameters as [3], which utilizes a 160-bit field for ECC to achieve the security level of 80 bits. For these settings, the random number is 20B, and an elliptic curve is 40B. Therefore, the pseudonym length is 56B, the signature length generated by BNN-IBS is 100B, and the signature length generated by the online offline signature scheme is 80B, as shown in Table 3. We chose the longest message at each stage for comparison. Table 5 lists the communication costs of the three schemes in different stages, where n is the number of certified vehicles.

Table 5. Communication costs of different schemes (byte).

Phase	ACPN	MADAR	EMAPP-Y	EMAPP-N
R2V	$64 + 92n$	$64 + 88n$	160	236
inner-V2V	112	156	180	236
cross-V2V	368	224	360	472

In Table 5, because ACPN and MADAR update the set of pseudonyms and offline signatures after each successful authentication, when the number of vehicles successfully authenticated increases continuously, their communication costs will also increase linearly. Our scheme gets rid of the set, so our scheme is more suitable for large-scale VANET and reduces the requirements for vehicle storage capabilities. Besides, as the signature generated by the signature scheme without linear pairing adopted in this evaluation is relatively long, the communication load is slightly increased.

7 Conclusion

In this paper, we propose a new mutual authentication framework EMAPP for VANET conditional privacy protection. The framework can improve efficiency without using expensive bilinear pairing and MTP, and it can use an identity-based signature scheme to achieve asymmetric mutual authentication between vehicles. Compared with [9,17], this framework can effectively resist Sybil attacks and impersonation attacks, and also reduce the requirements for car storage efficiency. In addition, through formal automated certification and comprehensive security analysis, we have proved that our scheme is safe and meets all security requirements. Performance evaluation shows that compared with [9,17], our framework also has higher efficiency in communication cost and computational load. As future work, we will explore how to reduce message length and further improve efficiency in terms of communication costs.

Acknowledgement. This work is supported in part by National Natural Science Foundation of China(Nos. 61572349, 61872262).

References

1. Armando, A., et al.: The AVISPA tool for the automated validation of internet security protocols and applications. In: Etessami, K., Rajamani, S.K. (eds.) CAV 2005. LNCS, vol. 3576, pp. 281–285. Springer, Heidelberg (2005). https://doi.org/10.1007/11513988_27
2. Bariah, L., Shehada, D., Salahat, E., Yeun, C.Y.: Recent advances in VANET security: a survey. In: 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), pp. 1–7, September 2015. https://doi.org/10.1109/VTCFall.2015.7391111

3. Chikhaoui, O., Ben Chehida Douss, A., Abassi, R., Guemara El Fatmi, S.: Towards the formal validation of a ticket-based authentication scheme for VANETS. In: 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 496–501, May 2018. https://doi.org/10.1109/WAINA.2018.00134
4. Chikhaoui, O., Chehida, A.B., Abassi, R., Fatmi, S.G.E.: A ticket-based authentication scheme for VANETs preserving privacy. In: Puliafito, A., Bruneo, D., Distefano, S., Longo, F. (eds.) ADHOC-NOW 2017. LNCS, vol. 10517, pp. 77–91. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-67910-5_7
5. Liu, D., Zhang, S., Zhong, H., Shi, R., Wang, Y.: An efficient identity-based online/offline signature scheme without key escrow. Int. J. Netw. Secur. **19**, 127–137 (2017). https://doi.org/10.6633/IJNS.201701.19(1).14
6. He, D., Zeadally, S., Xu, B., Huang, X.: An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Trans. Inf. Forensics Secur. **10**(12), 2681–2691 (2015). https://doi.org/10.1109/TIFS.2015.2473820
7. Horng, S.J., Tzeng, S.F., Huang, P.H., Wang, X., Li, T., Khan, K.: An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks. Inf. Sci. **317**, 48–66 (2015). https://doi.org/10.1016/j.ins.2015.04.033
8. Hubaux, J.P., Capkun, S., Luo, J.: The security and privacy of smart vehicles. IEEE Secur. Priv. **2**(3), 49–55 (2004). https://doi.org/10.1109/MSP.2004.26
9. Li, J., Lu, H., Guizani, M.: ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. IEEE Trans. Parallel Distrib. Syst. **26**(4), 938–948 (2015). https://doi.org/10.1109/TPDS.2014.2308215
10. Liu, X., Fang, Z., Shi, L.: Securing vehicular ad hoc networks. In: 2007 2nd International Conference on Pervasive Computing and Applications, pp. 424–429, July 2007. https://doi.org/10.1109/ICPCA.2007.4365481
11. Liu, Y., Wang, L., Chen, H.: Message authentication using proxy vehicles in vehicular ad hoc networks. IEEE Trans. Veh. Technol. **64**(8), 3697–3710 (2015). https://doi.org/10.1109/TVT.2014.2358633
12. Lu, R., Lin, X., Zhu, H., Ho, P., Shen, X.: ECPP: efficient conditional privacy preservation protocol for secure vehicular communications. In: IEEE INFOCOM 2008 - The 27th Conference on Computer Communications, pp. 1229–1237, April 2008. https://doi.org/10.1109/INFOCOM.2008.179
13. Bellare, M., Namprempre, C., Neven, G.: Security proofs for identity-based identification and signature schemes. J. Cryptol. **22**, 1–61 (2009). https://doi.org/10.1007/s00145-008-9028-8
14. Ming, Y., Cheng, H.: Efficient certificateless conditional privacy-preserving authentication scheme in VANETs. Mob. Inf. Syst. **2019**, 19 (2019). https://doi.org/10.1155/2019/7593138
15. Oh, H., Yae, C., Ahn, D., Cho, H.: 5.8 GHz DSRC packet communication system for ITS services. In: Gateway to 21st Century Communications Village. VTC 1999-Fall. IEEE VTS 50th Vehicular Technology Conference (Cat. No. 99CH36324), vol. 4, pp. 2223–2227, September 1999. https://doi.org/10.1109/VETECF.1999.797333
16. Yasmin, R., Ritter, E., Wang, G.: Provable security of a pairing-free one-pass authenticated key establishment protocol for wireless sensor networks. Int. J. Inf. Secur. **13**, 453–465 (2014). https://doi.org/10.1007/s10207-013-0224-7
17. Sun, C., Liu, J., Xu, X., Ma, J.: A privacy-preserving mutual authentication resisting DoS attacks in VANETs. IEEE Access **5**, 24012–24022 (2017). https://doi.org/10.1109/ACCESS.2017.2768499