IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 18, 2020, accepted August 31, 2020, date of publication September 3, 2020, date of current version September 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3021408

HPBS: A Hybrid Proxy Based Authentication Scheme in VANETs

HUA LIU, HAIJIANG WANG, AND HUIXIAN GU
School of Electronic and Information Engineering, Zhejiang University of Science and Technology, Hangzhou 310023, China

Corresponding author: Haijiang Wang (wanghaijiangyes@163.com)

This work was supported in part by the Natural Science Foundation of Zhejiang Province under Grant LQ20F020010.

ABSTRACT As a part of intelligent transportation, vehicle ad hoc networks (VANETs) have attracted the attention of industry and academia and have brought great convenience to drivers. As an open communication environment, any user can broadcast messages in the system. However, some of these users are malicious users and malicious users can broadcast false messages to interfere with the normal operation of the system. Therefore, we needed to authenticate the identity of the message sender. Currently, there are two main authentication methods in VANETs, one using public key infrastructure (PKI) to verify message integrity and sender identity, and the other using anonymous authentication schemes. Due to the high computational and transport overhead involved in validation, the certification efficiency of most existing schemes is not satisfactory. Therefore, these schemes are generally not applicable to real-world scenarios. In order to improve the efficiency of certification and satisfy the security requirements, in this paper, we proposed a hybrid proxy based authentication scheme (HPBS). In HPBS, by introducing the concept of agent vehicles and integrating identity-based and PKI-based hybrid authentication, we solved three problems in the VANETs environment: (1) improving the effectiveness of roadside units (RSUs) in terms of authenticating messages; (2) reducing the computational burden of RSUs; (3) protecting the privacy of users. The simulation results illustrate that the scheme not only ensures network security, but also greatly improves the efficiency of information verification.

INDEX TERMS Proxy vehicle, privacy, proxy based authentication, pseudonym, vehicular ad-hoc network.

I. INTRODUCTION

With the rapid development of artificial intelligence, wireless technology, automobiles and ad-hoc networks, the concepts of Intelligent Traffic System (ITS) and smart city have become more and more popular. In this context, the potential of vehicular ad hoc networks (VANETs) which can provide better driving services and road safety has attracted extensive attention from the government, academia and the business community. However, as an open communication environment, the security of VANETs communication has become an urgent problem to be solved [1].

In VANETs, vehicle-to-vehicle communication (V2V) and vehicle-to-infrastructure communication (V2I) are carried out in an open wireless channel environment. If we did not protect the communication properly [2], the personal privacy (geographical location, identity information and personal interests, etc.) of users will be easily acquired by attackers. Therefore, a message authentication scheme should be proposed to solve this problem.

Security issues in VANETs have been widely studied in many literatures [3]–[6]. However, except security problems, the efficiency of certification should not be ignored, which is one of the key reasons why VANETs can be deployed. According to the dedicated short-range communication (DSRC) protocol, each vehicle needs to broadcast a large amount of information periodically which includes the information of traffic conditions, vehicle speed, and service requests [7]. So, the message authentication scheme not only needs to satisfy security requirements, but also needs to be able to authenticate a large number of messages in a relatively short period of time.

At present, the existing authentication schemes [8]–[14] are mainly divided into two categories: the traditional public key infrastructure (PKI) scheme and the scheme based on identity. In traditional PKI schemes, the storage capacity of the vehicle is greatly required because enough pseudonyms and key pairs need to be distributed from certificate authority (CA). When vehicles send or receive messages, each message must be accompanied by a certificate, which greatly increases the overhead of transmission. When a vehicle is deregistered, the CA needs to put all the vehicle's pseudonymous

The associate editor coordinating the review of this manuscript and approving it for publication was Fan Zhang.

certificates on the certificate revocation list (CRL). As the number of unregistered vehicles increases, the CRL will accumulate indefinitely, which will result in obvious computational and transmission overhead.

The identity-based authentication scheme solves the problem of certificate management in PKI. However, this scheme greatly increases the computation and transmission costs of authentication [15]. In this scheme, each car has a large number of anonymous identities. When the vehicle needs to send a message, it needs to select a pseudonym to sign the message and send it. Therefore, the vehicle needs to have a large storage space to store the pseudonym. At the same time, the fact that a user has multiple anonymous identities increases a lot of computational overhead to the authority's tracking of real identities in case of communication disputes. To solve this problem, Zhang *et al.* [9] proposed an effective authentication based scheme that uses tamper-proof devices (TPD) to generate dynamic anonymous identities, which avoids the need for vehicles to store a large number of anonymous identities. At the same time, the login verification of TPD protects the user's personal privacy. In addition, this scheme uses RSU for batch authentication based on anonymous identity, which greatly reduces the computation and transmission costs of message authentication. However, the IBV scheme does not address V2V communication and is not resistant to replay attacks. And IBV scheme integrates information and authentication through RSU, which greatly increases the workload of RSU and reduces the efficiency of RSU authentication.

To solve these problems, in this paper, we proposed a proxy based hybrid authentication scheme (HPBS), which combines the PKI scheme and the identity-based anonymous batch authentication scheme and introduces the concept of proxy vehicle. During the system initialization phase, each agent vehicle and RSU receives a unique long term certificate from the CA. When the proxy vehicle enters the communication range of the new RSU, The proxy vehicle needs to be mutually verified with the RSU. At the end of authentication, the RSU and the proxy vehicle jointly generate a set of keys. In the group managed by the proxy vehicle, the message authentication of the ordinary vehicle is carried out using symmetric encryption with the group key as the key. When a proxy vehicle node or RSU node is compromised, the CA will revoke its unique certificate. Ordinary vehicles through the certificate of the proxy vehicle verify the validity of proxy vehicle. In V2I, we mainly used anonymous batch authentication based on identity twice. One is batch authentication of the agent vehicle to the ordinary vehicle, and the other is batch authentication of the RSU to the agent vehicle.

Specifically, our main contributions are as follows.

(1) We proposed a hybrid proxy based authentication scheme that satisfies the security and efficiency requirements of VANETs.

(2) Every RSU and proxy vehicle holds a long term PKI-based certificate, which is used to verify the validity of node. For the sent message, the vehicle needs to sign it with a locally generated pseudo-identity. The proxy vehicle and the RSU verify each other's certificates before they can communicate and generate group keys. Mutual authentication between vehicles can be quickly authenticated with group keys. The vehicle and RSU use bilinear batch authentication to authenticate the message.

(3) CA manages the revoked certificates by the RSU revocation lists (RCRL) and the proxy vehicle revocation lists (PVCRL). When the node registered in the list is corrupted, the CA can revoke its certificate. In view of the limited computing and storage resources of the RSU, we used the agent vehicle to decompress the RSU load.

The remainder of this paper is as follows: in section 2, we analyzed the relevant work of the existing literature. In section 3, we described the system model and preparation in detail. In section 4, we introduced the message authentication scheme proposed in this paper in detail. In section 5, we certified the safety of our program. In section 6, we analyzed and evaluated the performance of our solution in detail. In the last section, we summarized the research status and future work of this paper.

II. RELATED WORK

In VANETs, security authentication and privacy protection are two problems that need to be solved urgently. To solve these two problems, many anonymous authentication schemes [16]–[18] have been proposed. Most of them sign and authenticate messages based on PKI.

In order to protect the user's real identity and personal privacy, the concept of pseudonyms came into being. Chaum [19] established a pseudonymous system that allows entities to communicate effectively anonymously with other entities through pseudonyms. The proposed system plays a great role in protecting personal privacy. Fan *et al.* [20] solved the privacy protection and message authentication problems in vehicle communication systems, and proposed an efficient pseudonymy public key infrastructure (EPPKI) scheme using bilinear pairs. This scheme greatly improves the efficiency of message authentication. However, this scheme can not authenticate a large number of messages in a short time. In order to improve the security of the authentication system, Sun *et al.* [2] proposed an efficient anonymous authentication scheme based on bilinear pairings. However, the computational and transmission costs of this scheme are large. Yue *et al.* [21] proposed an anonymous authentication scheme based on group signature framework. The main advantage of this scheme is to improve the security of VANETs. However, the performance of this scheme still needs to be further improved.

In recent years, Zhang *et al.* [22] proposed an extensible vehicle anonymous batch authentication scheme that maintains the effectiveness of traditional schemes, reduces the size of CRL, and does not require the preloading of the same system private key. However, the scheme still requires large overhead in computation and storage.

To improve the efficiency of certification, in [23], Li *et al.* proposed a scheme for message authentication using secret sharing. The scheme uses verifiable secret sharing to verify each other and obtain a set of keys, and then uses this set of keys to generate and verify messages. This scheme has some advantages in performance. However, the scheme trusts the third party too much, and a single point of failure will cause the system to be completely destroyed.

Hasrouny *et al.* [24] proposed a group-based authentication scheme using elliptic curve cryptography (ECC). The scheme realizes the secure communication of V2V and reduces the delay caused by security message. The cost of validation is reduced because the recipient's certificate does not need to be validated. The scheme does not affect the efficiency of certification as the number of vehicles increases. However, the scheme does not take into account conditional privacy protection and batch authentication of messages. In [25], Shao *et al.* proposed an anonymous authentication scheme using bilinear pairs in distributed entity groups. This scheme adds the characteristics of threshold authentication on the basis of traditional anonymous authentication. The whole validation is based on batch authentication. However, for high-speed moving vehicles, the scheme will incur a lot of computing and communication costs, and the management of the certificate also has some problems. Gao *et al.* [26] proposed a virtual network privacy protection scheme based on pseudonym ring in order to solve the problems of ring establishment and ring member selection. The scheme has a deep network structure and a trust model. Compared with the traditional scheme, the scheme has stronger robustness and efficiency. In [27], Liu *et al.* proposed a practical distributed condition security authentication scheme. The scheme does not need to rely on TPD and has a significant improvement in security features. In [28], Mamun and Miyaji proposed a scheme based on bilinear pairings.This scheme improves batch authentication of identification-based Group Signature (IBGS). The scheme improves the original scheme by batch scheduling algorithm, which improves the performance of authentication. However, performance results for the scheme are not provided.

III. SYSTEM MODEL AND PRELIMINARIES

In this section, We introduced our system model in detail and briefly list the basic theoretical knowledge for our solution.

A. SYSTEM MODEL

At present, most studies [11] [29], [30] solve the VANET authentication problem through the two-layer network model. The two-layer network model is the management layer and the application layer respectively. The application layer is generally composed of vehicles and RSUs, which communicate with each other through the wireless DSRC channel. And vehicles are divided into group leader vehicles and general vehicles. Management consists of CA and application server (AS) who communicate with RSU via the Internet. In particular, the communication types can be divided into V2V and V2I, as shown in FIGURE 1.

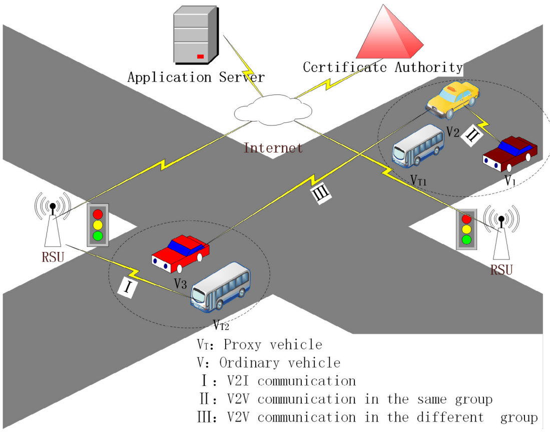


FIGURE 1. The system model of VANETs.

(1) V_T: On the road, there are many buses that run a fixed route every day. We chose these buses with fixed routes and large computing and storage resources as our proxy vehicles. In Figure 1, V_T is the proxy vehicle we chose. First, it needs to authenticate with the RSU and generate an in-group key. Secondly, it is also responsible for collecting and sorting out the authentication information of the surrounding vehicles, then verifying the time stamp, and finally integrating the verified information and handing it to the RSU for batch authentication.

(2) CA: CA is the trusted agency for the entire system. It is responsible for assigning long-term certificates to proxy vehicle nodes. All proxy vehicles and RSUs must be registered with CA before joining VANETs. It is maintained by CRL respectively. We assume that the CA has sufficient computing power and storage capacity for communication, and that it cannot be breached by any adversary.

(3) RSU: RSU connects management to the application layer. On the one hand, the RSU is responsible for checking the validity of the proxy vehicle certificate entering its communication range and providing the group key to the V_T. On the other hand. The RSU is responsible for the bilinear batch authentication based on false identity for the group member authentication information sorted out by V_T. Bilinear authentication based on false identity is performed for discrete common vehicles that are not in the group.

(4) On board Unit (OBU): OBU is a device that is built into the vehicle during production. OBU can communicate not only with other OBUs, but also with RSUs. In this scheme, we assume that each OBU is equipped with a TPD.

B. BILINEAR MAPS

Let G be a cyclic additive group and G_M be a cyclic multiplicative group. The point $P \in G$ generates the group G. G and G_M have the same prime order q, $|G| = |GM| = q$. Let $e : G \times G \rightarrow G_M$ be a bilinear pairing which satisfies three flowing properties [32, 33].

(1) Bilinearity: For all $P, T, S \in G$, $e(P + T, S) = e(P, S)e(T, S)$ and $e(P, T+S) = e(P, T)e(P, S)$. In particular, for all $a, b \in Z_q^*$, $e(aP, bP) = e(P, P)^{ab} = e(P, abP) = e(abP, P)$.

(2) Non-degenerate: There exist two points $P, T \in G$ such that $e(P, T) \neq 1$, where 1 is the identity element in G_M.

(3) Computability: There must is an efficient algorithm to compute $e(P, T)$ for all $P, T \in G$.

In bilinear groups with mapping e, DDH problem is easy to calculate, while CDH problem is difficult to calculate [33]. For example, for any $x, y \in Z_q^*$, and given $xP, yP, xyP \in G$, there exists an efficient algorithm to checking $e(xP, yP) = e(P, xyP)$.

C. SECURITY REQUIREMENTS

The vehicle-to-All communication (V2X) scenario mainly satisfies to meet three security requirements: identity privacy protection, message authentication and traceability. We will discuss this in more detail below.

Message authentication: In V2X communication, authentication must be performed to ensure that the message has not been changed by the legal entity and is delivered in the communication. In addition, on heavily traffic-intensive routes, we need to make certification more efficient to avoid system crashes.

Identity privacy preserving: In V2X communication system, because of its broadcast nature, the information of specific identity will be monitored frequently. If the signature scheme used is a normal signature scheme, this can easily reveal the identity of the individual [34]. Even if we use a pseudonym for signature, an attacker can still link to a car by analyzing multiple signatures.This can lead to a loss of location privacy [35]. Therefore, identity privacy needs to be protected.

Traceability: When the signature is disputed or the message content is forged, the CA should be able to retrieve the vehicle's real identity from the vehicle's false identity.

IV. A HYBRID PROXY BASED AUTHENTICATION SCHEME

In this paper, we proposed a hybrid proxy based authentication scheme, which uses identity-based signature and the PKI-based certificate. Here, the certificate is mainly used to verify the identity of RSU nodes and V_T nodes. The identity-based signature is mainly used for anonymous identity-based batch authentication of vehicles in the group and anonymous identity-based single authentication of discrete vehicles outside the group. The process of our scheme mainly includes the following five steps: the basic idea of the scheme, the initialization of the system, the generation of group key, the authentication of signature and the tracking of real identity. The symbols used in this article are listed in Table 1.

A. BASIC IDEAS

In this section, we introduced the idea of our scheme in the paper, as shown in FIGURE 2.

In VANETs, CA is the only organization used to register certificates and issue certificates. RSU and V_T are registered in the CA for long term certificates, which are put into their OBU. Particularly, we let the CA manage revocation certificates for the RSU and vehicle, respectively. That is, when the RSU and V_T are revoked, their certificates are added to the CRL, respectively. When the RSU and V_T need to be authenticated, other entities can query the status of the certificates they provide through Online Certificate Status Protocol (OCSP) and authenticate them with the public key in the certificate.

TABLE 1. Notation.

Notation	Descriptions
CA	A certificate authority
AS	A application server
V_i	The ith vehicle
V_T	The ith proxy vehicle
RSU	A roadside unit
G	A cyclic additive group
G_M	A cyclic multiplicative group
P	The generator of the cyclic additive group G
e	A bilinear map: $G \times G \rightarrow G_M$
q	The order of the group G
N	A random nonce
d^j	The ith private master key of the tamper-proof device, where j is equal to 1 or 2
$P_{pub_i^j}$	The ith public key of the CA, where j is equal to 1 or 2
SK_{CA}, PK_{CA}	The private and public key of CA
$Cert_{CA,R}$	The certificate of RSU
SK_R, PK_R	The private and public key of RSU
SK_T, PK_T	The private and public key of vehicle V_T
$Cert_{CA,T}$	The certificate of vehicle V_T
RID	The real identity of the vehicle
PWD	A password or authentication credential used to activate a tamper-proof device
AID	A pseudo identity of the vehicle V
AID^j	A part of the AID, such that AID=(AID^1, AID^2)
SK	A private key of the vehicle V
SK^i	A part of the SK, such that SK=(SK^1, SK^2)
PSK	The identity of a group
M	A message
h	A one-way hash function such that SHA-1
H	A MapToPoint hash function such as $H : 0, 1^* \rightarrow G$
$\|$	Message concatenation operation, which appends several messages together in a special format
$\bigoplus$	The xor operation
Msg_{V_T}	The message sent by V_T
Msg_R	The message sent by RSU

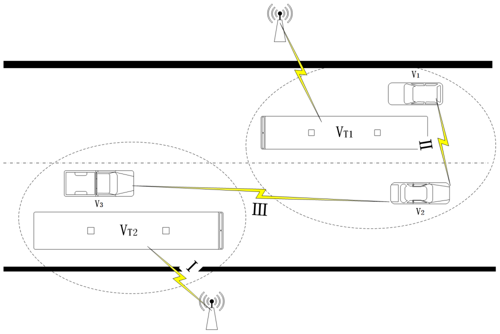


FIGURE 2. The system model of VANETs.

Both the RSU and V_T periodically broadcast a hello message, including its own public key, certificate, and so on.

The RSU works as follows. When a vehicle enters the RSU communication range to send a message to the RSU, the RSU will judge the message it sends. If the communication vehicle is V_T, the in-group key will be generated after being authenticated with V_T, and the messages of all members sorted out by V_T will be authenticated with bilinear batch based on anonymous identity. If the communication vehicle is a

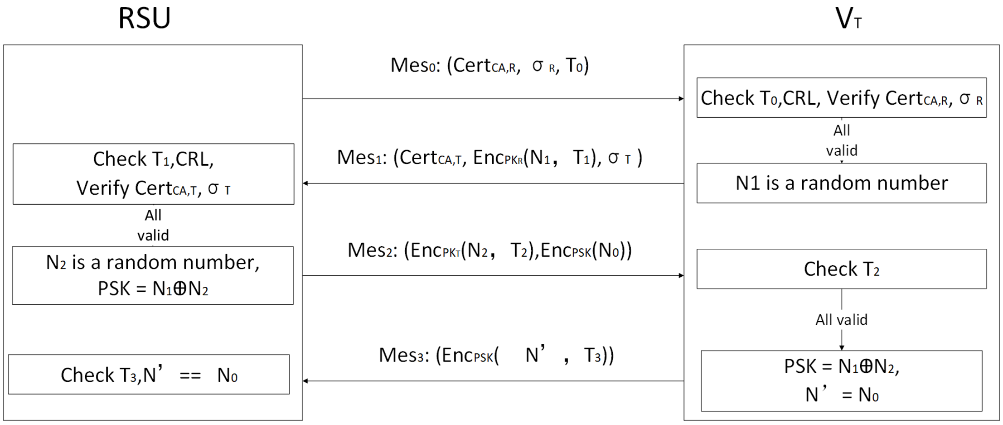

RSU
V_T
Mes_0: ($Cert_{CA,R}$, σ_R, T_0)
Check T_0,CRL, Verify $Cert_{CA,R}$, σ_R
All valid
N1 is a random number
Mes_1: ($Cert_{CA,T}$, Enc_{PK_R}(N_1, T_1), σ_T)
Check T_1,CRL, Verify $Cert_{CA,T}$, σ_T
All valid
N_2 is a random number, PSK = $N_1 \oplus N_2$
Mes_2: (Enc_{PK_T}(N_2, T_2),Enc_{PSK}(N_0))
Check T_2
All valid
PSK = $N_1 \oplus N_2$, N' = N_0
Mes_3: (Enc_{PSK}(N' , T_3))
Check T_3,N' == N_0

FIGURE 3. **The identity of a group.**

normal vehicle, only a single bilinear authentication based on anonymous identity is performed for the message.

As V_T, each time it enters the communication range of the RSU, it first authenticates with the RSU and obtains the key within the group. V_T also needs to collate messages from group members and send them to the RSU.

If the ordinary vehicle can find V_T within the communication range, the V_T is authenticated, and then the message that needs to be sent to the RSU is sent to V_T after successful authentication. If V_T does not exist within the communication range, the vehicle authenticates the RSU directly and sends a message.

In our scheme, we also had V2V communication. We divided V2V into two groups: V2V communication between two groups and vehicle communication within the group and discrete vehicle communication outside the group.

B. SYSTEM INITIALIZATION

The CA initializes the system parameters and assigns certificates to each RSU node and V_T node.The system initialization process is as follows:

1) SYSTEM PARAMETER GENERATION

The CA as a trust institution that checks the vehicle's identity and generates and pre-distributes the vehicle's private key. During system initialization, the CA sets the following system parameters for each RSU and OBU:

(1) G is a cyclic addition group of order q generated by P, and G_M is the same group of multiplication cycles as G. Let $e : G \times G \rightarrow G_M$ be a bilinear map.

(2) CA selects a random number $c \in Z_q^*$ as its private key SK_{CA}, and then Calculate the public key $PK_{CA} = SK_{CA}P$.

(3) CA first randomly selected $d^1, d^2 \in Z_q^*$ as the two private keys, and calculated the corresponding public keys $P_{pub^1} = d^1P$, $P_{pub^2} = d^2P$. The CA puts the two keys into each vehicle's TPD.

(4) Each RSU node and OBU node is equipped with a public parameter $\{G, G_M, P, q, PK_{CA}, P_{pub^1}, P_{pub^2}, h, H, e\}$, and each vehicle's TPD is equipped with a parameter $\{d^1, d^2\}$.

(5) The RID and PWD are required for the vehicle to start TPD. The RID is the unique identification of the vehicle, and the PWD is the password required to start TPD.

2) RSU CERTIFICATE ISSUANCE

For each RSU, the certificate and RSU key pair are generated when the RSU is registered. The process is as follows:

(1) CA randomly selected a number $t \in Z_q^*$ as RSU's private key SK_R, and calculated RSU's public key $PK_R = tP$.

(2) The CA signs PK_R and generates the certificate $Cert_{CA,R} = \{PK_R, \sigma_{CA}\}$ and sends it to RSU for saving through a secure channel. And $\sigma_{CA} = sign_{PK_{CA}}(PK_R)$.

3) V_T CERTIFICATE ISSUANCE

For each V_T, the certificate and V_T key pair are generated when the V_T is registered.The process is as follows:

(1) CA randomly selected a number $l \in Z_q^*$ as V_T's private key SK_T, and calculated V_T's public key $PK_T = lP$.

(2) The CA signs PK_T and generates the certificate $Cert_{CA,T} = \{PK_T, \sigma_{CA}\}$ and sends it to V_T for saving through a secure channel. And $\sigma_{CA} = sign_{PK_{CA}}(PK_T)$.

C. THE IDENTITY OF A GROUP GENERATION AND ANONYMOUS IDENTITY GENERATION

The RSU broadcasts within its communication range.When a vehicle is communicating with it, the RSU detects if the vehicle is V_T. If so, the RSU and V_T jointly generate the group key of V_T. The detail can be described as FIGURE 3.

1) THE IDENTITY OF A GROUP GENERATION

(1) RSU broadcasts message Mes_0:$\{Cert_{CA,R}, \sigma_R, T_0\}$ within the communication range, where $Cert_{CA,R} = \{PK_R, \sigma_{CA}\}$, $\sigma_R = sign_{PK_R}('hello')$ and T_0 is a timestamp.

(2) After receiving Mes_0, V_T first checks the status of $Cert_{CA,R}$ with OCSP, then checks the timestamp T_0 and verifies the certificate $Cert_{CA,R}$ and the signature σ_R. When all validation is passed, V_T generates a random number N_1 and sends Mes_1:$\{Cert_{CA,T}, Enc_{PK_R}(N_1), T_1, \sigma_T\}$ to the RSU. And $Cert_{CA,T} = \{PK_T, \sigma_{CA}\}$, $\sigma_{CA} = sign_{PK_{CA}}(PK_T)$.

(3) After receiving Mes_1, RSU first checks the status of $Cert_{CA,T}$ with OCSP, then checks the timestamp T_1 and verifies the certificate $Cert_{CA,T}$ and the signature σ_T. When all validation is passed, RSU generates a random number N_2 and computes $PSK = N_1 \bigoplus N_2$. RSU sends information Mes_2:$\{Enc_{PK_T}(N_2, T_2), Enc_{PSK}(N_0)\}$ to V_T.

Algorithm 1 The Identity of a Group Generation

```
RSU broadcast $Mes_0$:{$Cert_{CA,R}$, $\sigma_R$, $T_0$}
$V_T$ receive $Mes_0$
Check $T_0$, $Cert_{CA,R}$, $\sigma_R$
if $T_0$,$Cert_{CA,R}$ and $\sigma_R$ are valid then
    $V_T$ generates a random number $N_1$
    $V_T$ send $Mes_1$:{$Cert_{CA,T}$, $Enc_{PK_R}(N_1)$, $T_1$, $\sigma_T$} to the RSU
    RSU receive $Mes_1$
    Check $T_1$, $Cert_{CA,T}$, $\sigma_T$
    if $T_1$,$Cert_{CA,T}$ and $\sigma_T$ are valid then
        RSU generates a random number N2 and computes PSK = $N_1 \oplus N_2$
        RSU sends $Mes_2$ : $Enc_{PK_T}(N_2, T_2)$, $Enc_{PSK}(N_0)$ to $V_T$
        $V_T$ receive $Mes_2$
        $V_T$ checks $T_2$
        if $T_2$ are valid then
            $V_T$ calculate PSK = $N1 \oplus N2$
            $V_T$ send $Mes_3$ : {$Enc_{PSK}(N_0, T_3)$} to the RSU
            RSU receive $Mes_3$
            Check $N_0$, $T_3$
            if $T_2$ and $T_3$ are valid then
                The group key generation ends
else if then
```

(4) V_T checks T_2. If the check passes, calculate $PSK = N_1 \bigoplus N_2$, $N' = N_0$ and send Mes_3 to the RSU. RSU verifies T_3 and N', The group key generation ends when the validation passes.

The specific algorithm of group key generation is shown in Algorithm 1.

Here, we used the RSU and the proxy vehicle to generate identity of a group for each proxy vehicle's group. The identification of group identity is mainly used to distinguish the communication between groups in V2V communication. In Section 4.4.2, we went into detail.

2) ANONYMOUS IDENTITY GENERATION

All vehicles use the parameters given when the CA is registered and the TPD device to generate their respective anonymous identities. The process is as follows.

In order to protect the privacy of users, we used TPD to generate false identities and corresponding private keys [31]. TPD is mainly composed of the following parts: authentication module, pseudo-identity generation module, and private key generation module. These three modules are described in detail below.

Authentication module: The identity module is an access control module for TPD, and only if you have RID and PWD can you start the device. PWD is the CA's signature to RID. Pass the verification of this module and go to the next module. Here, we assumed that TPD is unbeatable.

Pseudo identity generation module: This module is mainly used to generate pseudo-identities for RID, and each pseudo-identity AID consists of AID^1 and AID^2. In this module, the ElGamal encryption algorithm [36] over the ECC [37] is employed to generate pseudonyms. And $AID^1 = N \cdot P$, $AID^2 = RID \bigoplus H(N \cdot P_{pub^1})$, where N is a random nonce. Each pseudo-identity is guaranteed to be unique by every change of N. Here, P and P_{pub1} are the public parameters for the CA preload. AID^1 and AID^2 are generated and passed to the next module.

Private key generation module: This module uses identity-based encryption [32]. This module is mainly used to generate the private key SK, which consists of two parts, SK^1 and SK^2, where $SK^1 = d^1 \cdot AID^1$ and $SK^2 = d^2 \cdot H(AID^1 \parallel AID^2)$, respectively.

Finally, the vehicle can obtain a list of pseudo-identities $AID = (AID^1, AID^2)$ and the corresponding private key $SK = (SK^1, SK^2)$.

D. SIGNATURE VERIFICATION

1) MESSAGE SIGNING

According to the DSRC agreement, vehicles on the road need to periodically broadcast traffic-related information, because these transmitted information may affect the traffic control center's reasonable command of the traffic and make a correct judgment of the current traffic situation. Therefore, we needed to sign the sent message anonymously to improve the security of communication. The sender can protect its own privacy, and the recipient can verify the integrity and validity of the message by signing. The specific algorithm process is shown in TABLE 2. Details of the signature are as follows.

(1) First, the vehicle V_i generates a daily traffic information m_i.

(2) V_i selects an anonymous identity and the corresponding private key to sign the message $M_i = m_i \parallel T_i$, where the signature $\sigma_i = SK_i^1 + h(M_i)SK_i^2$.

(3) V_i broadcasts the message (AID_i, M_i, σ_i), where $AIDi = (AID_i^1, AID_i^2)$ and $\sigma_i = SK_i^1 + h(M_i)SK_i^2$.

(4) These steps are repeated every 100-300 ms according to the DSRC [38].

2) MESSAGE VERIFICATION

In message authentication, we mainly divided into three authentication methods. The vehicles in the group communicate with the RSU, Vehicles in the same group communicate with each other, Vehicles that are not in the same group communicate with each other.

(1) The vehicles in the group communicate with the RSU: Given the system public parameters: we used bilinear message authentication based on anonymous identity. $\{G, G_M, P, q, PK_{CA}, P_{pub_i^1}, P_{pub_i^2}, h, H, e\}$ and the message (AID_i, M_i, σ_i) sent by discrete vehicle V_i. Each V_T first batch authenticates message (AID_i, M_i, σ_i) for a member of the group. V_T needs to validate $e(\sum_{i=1}^{n} \sigma_i, P)$ $= e(\sum_{i=1}^{n} AID_i,\ P_{pub_i^1})\, e(\sum_{i=1}^{n} h(M_i)\ HAID_i, P_{pub_i^2})$, where

TABLE 2. The specific algorithm of the scheme.

V_i	V_T	RSU
Input: RID, PWD		
$AID^1 = N \cdot P$		
$AID^2 = RID \oplus H(N \cdot P_{pub^1})$		
$SK^1 = d^1 \cdot AID^1$		
$SK^2 = d^2 \cdot H(AID^1 \parallel AID^2)$		
$SK = (SK^1, SK^2)$		
$M_i = m_i \parallel T_i$		
$AID_i = (AID_i^1, AID_i^2)$		
$\sigma_i = SK_i^1 + h(M_i)SK_i^2$		
$SendAID_i, M_i, \sigma_i$ to V_T		
	Input:$\{G, G_M, P, q, PK_{CA}, P_{pub_i^1}, P_{pub_i^2}, h, H, e\}$	
	$HAID_i = H(AID_i^1 \parallel AID_i^2)$	
	$e(\sum_{i=1}^n \sigma_i, P)? =$	
	$e(\sum_{i=1}^n AID_i, P_{pub_i^1})e(\sum_{i=1}^n h(M_i)HAID_i, P_{pub_i^2})$	
	$M_T = (\sum_{i=1}^n m_i) \parallel T_T$	
	$\sigma_T = SK_T^1 + h(M_T)SK_T^2$	
	Send (AID_T, M_T, σ_T) to the RSU	
		Input:$\{G, G_M, P, q, PK_{CA}, P_{pub_T^1}, P_{pub_T^2}, h, H, e\}$
		Check T_T
		If T_T is valid
		Then $e(\sigma_T, P)? =$
		$e(AID_T^1, P_{pub_T^1})e(h(M_T)H(AID_T^1 \parallel AID_i^2), P_{pub_T^2})$
		Message verification completed

$HAID_i = H(AID_i^1 \parallel AID_i^2)$. This batch verification equation follows since.

$$\begin{aligned}
&e(\sum_{i=1}^{n} \sigma_i, P)\\
&= e(\sum_{i=1}^{n}(SK_i^1 + h(M_i)SK_i^2), P)\\
&= e(\sum_{i=1}^{n} SK_i^1, P)e(\sum_{i=1}^{n} h(M_i)SK_i^2, P)\\
&= e(\sum_{i=1}^{n} d_i^1 AID_i^1, P)e(\sum_{i=1}^{n} d_i^2 h(M_i)HAID_i, P)\\
&= e(\sum_{i=1}^{n} AID_i^1, d_i^1 P)e(\sum_{i=1}^{n} h(M_i)HAID_i, d_i^2 P)\\
&= e(\sum_{i=1}^{n} AID_i^1, P_{pub_i^1})e(\sum_{i=1}^{n} h(M_i)HAID_i, P_{pub_i^2})
\end{aligned}$$

V_T will consolidate the message that the authentication is successful and the timestamp is normal into $M_T = (\sum_{i=1}^n m_i) \parallel T_T$ and send (AID_T, M_T, σ_T) to the RSU. T_T is a timestamp and $\sigma_T = SK_T^1 + h(M_T)SK_T^2$. The RSU validates $e(\sigma_T, P) = e(AID_T^1, P_{pub_T^1})e(h(M_T)H(AID_T^1 \parallel AID_i^2), P_{pub_T^2})$, as verified below.

$$\begin{aligned}
&e(\sigma_T, P)\\
&= e(SK_T^1 + h(M_T)SK_T^2, P)\\
&= e(SK_T^1, P)e(h(M_T)SK_T^2, P)\\
&= e(d_T^1 AID_T^1, P)e(h(M_T)d_T^2 H(AID_T^1 \parallel AID_T^2), P)\\
&= e(AID_T^1, d_T^1 P)e(h(M_T)H(AID_T^1 \parallel AID_T^2), d_T^2 P)\\
&= e(AID_T^1, P_{pub_T^1})e(h(M_T)H(AID_T^1 \parallel AID_T^2), P_{pub_T^2})
\end{aligned}$$

(2) Vehicles in the same group communicate with each other: we used bilinear message authentication based on anonymous identity. One of the vehicles sends a message $(AID_i, M_i, \sigma_i, PSK_i)$ to the other vehicle. If PSK_i is the same as your own PSK, then this information comes from the same group of vehicles. The signature σ_i is valid if $e(\sigma_i, P) = e(AID_i^1, P_{pub_i^1})e(h(M_i)H(AID_i^1 \parallel AID_i^2), P_{pub_i^2})$, as verified below.

$$\begin{aligned}
&e(\sigma_i, P)\\
&= e(SK_i^1 + h(M_i)SK_i^2, P)\\
&= e(SK_i^1, P)e(h(M_i)SK_i^2, P)\\
&= e(d_i^1 AID_i^1, P)e(h(M_i)d_i^2 H(AID_i^1 \parallel AID_i^2), P)\\
&= e(AID_i^1, d_i^1 P)e(h(M_i)H(AID_i^1 \parallel AID_i^2), d_i^2 P)\\
&= e(AID_i^1, P_{pub_i^1})e(h(M_i)H(AID_i^1 \parallel AID_i^2), P_{pub_i^2})
\end{aligned}$$

(3) Vehicles that are not in the same group communicate with each other: Here, we used bilinear message authentication based on anonymous identity. One of the vehicles sends a message (AID_i, M_i, σ_i) to the other vehicle, the signature σ_i is valid if $e(\sigma_i, P) = e(AID_i^1, P_{pub_i^1})e(h(M_i)H(AID_i^1 \parallel AID_i^2), P_{pub_i^2})$, as verified below.

$$\begin{aligned}
&e(\sigma_i, P)\\
&= e(SK_i^1 + h(M_i)SK_i^2, P)\\
&= e(SK_i^1, P)e(h(M_i)SK_i^2, P)\\
&= e(d_i^1 AID_i^1, P)e(h(M_i)d_i^2 H(AID_i^1 \parallel AID_i^2), P)\\
&= e(AID_i^1, d_i^1 P)e(h(M_i)H(AID_i^1 \parallel AID_i^2), d_i^2 P)\\
&= e(AID_i^1, P_{pub_i^1})e(h(M_i)H(AID_i^1 \parallel AID_i^2), P_{pub_i^2})
\end{aligned}$$

Through the above four authentication methods, we will introduced the V2I and V2V message authentication methods in our system.

First of all, we used V_T and RSU to achieve batch certification on dense traffic roads in our scheme, which greatly reduces the certification delay. We mixed in the PKI scheme and used certificates to guarantee the identity of RSU and V_T, which improved the security of the whole system. We also used pseudonyms to protect users' privacy. We used V_T to integrate the information and send a timestamp to the RSU for authentication, which not only prevented replay attacks, but also relieved the pressure on the RSU to authenticate and integrate the information at the same time.

In addition, in the authentication of intra-group communication, we used the authentication scheme based on symmetric key, which greatly reduces the authentication time of intra-group information, improves the rate of intra-group communication, and guarantees the security of communication.

V. SECURITY ANALYSIS

This section will mainly analyze the security of our proposed scheme. Firstly, BAN Logic is adopted to prove the correctness of the scheme. Secondly, we apply informal security analysis to illustrate the security requirements our solution meets.

A. PROOF OF SAFETY

In this section, we use BAN Logic in [39] to prove the logical correctness of HPBS scheme. BAN logic is a formal logic widely used for reasoning about encryption and protocols.The BAN logic can be used to prove that the protocol implementation is achieving the desired goal.At the same time, we can also use it to find some defects in the scheme design.

The HPBS programme has two main objectives. One is that during authentication, V_T and RSU determine that they share a new session key. The other goal is for V_T and RSU to get information from each other.

With X as V_i, Y and Z as RSU, M_A and M_B as P^a and P^b, D_A as Msg_{V_T}, D_B and D_C as Msg_R, K_A and K_A^{-1} as PK_T and SK_T, K_B and K_B^{-1} as PK_R and SK_R, T_{A1}, T_B, T_{A2} and T_C as the timestamp, K_{AB} as PSK, the messages in the HPBS scheme can be represented as follows:

$V_T \rightarrow RSU$:

$X \rightarrow Y$:

$T_{A1}, Y, X, \{M_A, D_A\}_{K_B}, \{T_{A1}, Y, X, \{M_A, D_A\}KB\}_{K_A^{-1}}$

$RSU \rightarrow V_T$:

$Y \rightarrow X$:

$T_B, X, Y, \{M_B, D_B\}_{K_A}, \{T_B, X, Y, \{M_B, D_B\}KA\}_{K_B^{-1}}$

$V_T \rightarrow RSU$:

$X \rightarrow Z : T_{A2}, Z, X, \{T_{A2}, Z, X\}K_{AB}$

$RSU \rightarrow V_T$:

$Z \rightarrow X : T_C, X, Z, \{T_C, X, Z, D_C\}K_{AB}$

As a plaintext can be easily forged, the idealized message in BAN logic is shown as follows:

$V_T \rightarrow RSU$:

$X \rightarrow Y : \{M_A, D_A\}_{K_B}, \{T_{A1}, Y, X, \{M_A, D_A\}KB\}_{K_A^{-1}}$

$RSU \rightarrow V_T$:

$Y \rightarrow X : \{M_B, D_B\}_{K_A}, \{T_B, X, Y, \{M_B, D_B\}KA\}_{K_B^{-1}}$

$V_T \rightarrow RSU$:

$X \rightarrow Z : \{T_{A2}, Z, X\}K_{AB}$

$RSU \rightarrow V_T$:

$Z \rightarrow X : \{T_C, X, Z, D_C\}K_{AB}$

As both of V_T and RSU use their IDs as their public keys and broadcast to neighbors, it can be assumed that:

$X \mid\equiv (K_A) \mapsto X\ X \mid\equiv (K_B) \mapsto Y\ Y \mid\equiv (K_B) \mapsto Y$

$Y \mid\equiv \sharp(T_{A1})\ X \mid\equiv \sharp(T_B)\ Z \mid\equiv \sharp(T_{A2})\ X \mid\equiv \sharp(T_C)$

$X \mid\equiv \sharp(M_A)\ Y \mid\equiv \sharp(M_B)\ Y \mid\equiv \sharp(D_B)\ Z \mid\equiv \sharp(D_C)$

Through the logic of BAN, we obtain:

$$\frac{Y \mid\equiv (K_A) \mapsto X, Y \triangleleft \{T_{A1}, Y, X, \{M_A, D_A\}_{K_B}\}_{K_A^{-1}}}{Y \mid\equiv X \mid\sim (T_{A1}, Y, X, \{M_A, D_A\}_{K_B})}$$

Using T_{A1} for fresh rule, we derive:

$$\frac{Y \mid\equiv \sharp(T_{A1})}{Y \mid\equiv \sharp(T_{A1}, Y, X, \{M_A, D_A\}K_B)}$$

Furthermore, with nonce-verification rule, we can infer:

$$\frac{Y \mid\equiv \sharp(T_{A1}, Y, X, \{M_A, D_A\}_{K_B}), Y \mid\equiv X \mid\sim (T_{A1}, Y, X, \{M_A, D_A\}_{K_B})}{Y \mid\equiv X \mid\equiv (M_A, D_A)}$$

From $RSU \rightarrow V_T$, via the message-meaning, we also obtain:

$$\frac{X \mid\equiv (K_B) \mapsto Y, X \triangleleft \{T_B, X, Y, \{M_B, D_B\}_{K_A}\}_{K_B^{-1}}}{X \mid\equiv Y \mid\sim (T_B, X, Y, \{M_B, D_B\}_{K_A})}$$

Using T_B for fresh rule, we obtain:

$$\frac{X \mid\equiv \sharp(T_B)}{X \mid\equiv \sharp(TB, X, Y, \{M_B, D_B\}_{K_A})}$$

So, with nonce-verification rule,we obtain:

$$\frac{X \mid\equiv \sharp(T_B, X, Y, \{M_B, D_B\}_{K_A}), Y \mid\equiv X \mid\sim (T_B, X, Y, \{M_B, D_B\}_{K_A})}{X \mid\equiv Y \mid\equiv (M_B, D_B)}$$

With K_{AB}, we can obtain:

$$\frac{X \mid\equiv Y \mid\equiv (M_B, D_B), Y \mid\equiv X \mid\equiv (M_A, D_A)}{X \mid\equiv Y \mid\equiv X(K_{AB}) \leftrightarrow Y, Y \mid\equiv X \mid\equiv X(K_{AB}) \leftrightarrow Y}$$

From the above equation, we can see the authentication process between V_T and RSU, which means that the HPBS case can meet the first security objective.

From $V_T \rightarrow RSU$, we obtain:

$$\frac{Z \mid\equiv X(K_{AB}) \leftrightarrow Z, X \triangleleft \{T_{A2}, Z, X\}_{K_{AB}}}{Z \mid\equiv X \mid\sim (\{T_{A2}, Z, X\}_{K_{AB}})}$$

Using T_{A2} for fresh rule, we also derive:

$$\frac{Z \mid\equiv \sharp(T_{A2})}{Z \mid\equiv \sharp(\{T_{A2}, Z, X\}_{K_{AB}})}$$

Therefore, we can derive by nonce-verification rule:

$$\frac{Z \mid\equiv \sharp(\{T_{A2}, Z, X\}_{K_{AB}}), Z \mid\equiv X \mid\sim (\{T_{A2}, Z, X\}_{K_{AB}})}{Z \mid\equiv A \mid\equiv (T_{A2}, Z, X)}$$

From $V_T \rightarrow RSU$,via the message-meaning, we obtain:

$$\frac{X \mid\equiv X(K_{AB}) \leftrightarrow Z, Z \triangleleft \{T_C, X, Z, D_C\}_{K_{AB}}}{X \mid\equiv Z \mid\sim (\{T_C, X, Z, D_C\}_{K_{AB}})}$$

In addition, using T_C for fresh rule, we get:

$$\frac{X \mid\equiv \sharp(T_C)}{X \mid\equiv (\{T_C, X, Z, D_C\}_{K_{AB}})}$$

Finally, with nonce-verification rule, we can derive:

$$\frac{X \mid\equiv \sharp(\{T_C, X, Z, D_C\}_{K_{AB}}), Z \mid\equiv X \mid\sim (\{T_C, X, Z, D_C\}_{K_{AB}})}{X \mid\equiv Z \mid\equiv (T_C, X, Z, D_C)}$$

It can be determined from the above proof that the HPBS program can also fulfill the second goal. Through the formal proof of HPBS scheme, we can conclude that the scheme can guarantee the integrity of the information exchanged and the confidentiality of the recipient.

B. THE FORMAL SECURITY ANALYSIS

In this section, we mainly proved the security of our scheme from four aspects: the message authentication, the user identity privacy preservation, the resist replay attacks, and the traceability by the CA.

1) THE MESSAGE AUTHENTICATION

The message authentication is the basic security requirements of VANETs. In our scheme, the signature $\sigma_i = SK_i^1 + h(M_i)SK_i^2$ is actually a one-time identity-based signature. It is impossible to forge a valid signature without knowing SK_i^1 and SK_i^2. Because of the NP-hard computation complexity of Diffie-Hellman problem in G, it is difficult to derive the private keys SK_i^1 and SK_i^2 by way of AID_i^1, $P_{pub_i^1}$, P, and $H(AID_i^1 \parallel AID_i^2)$. On the other hand, $\sigma_i = SK_i^1 + h(M_i)SK_i^2$ is a diophantine equation, and we knew that just knowing σ_i and $h(M_i)$ to get SK_i^1 and SK_i^2 is quite difficult.

On the other hand, the CA assigns long-term certificates to each registered RSU and V_T. When V_T and RSU authenticate each other's messages, we used pki-based certificate authentication. We can authenticated the message by verifying the status of the certificate.

Therefore, we can concluded that the one-time identity-based signature in our scheme is secure as message authentication.

2) THE USER IDENTITY PRIVACY PRESERVATION

In our scheme, we generated two random pseudo-identities AID_i^1 and AID_i^2 using the real identity RID_i of the vehicle i and the random number N, where $AID_i^1 = NP$ and $AID_i^2 = RID_i \bigoplus H(NP_{pub_i^1})$. Because the pseudo-identity pair (AID_i^1, AID_i^2) is an ElGamaltype ciphertext, it can resist the opt-in plaintext attack. Therefore, without knowing the key pair (s_i^1, s_i^2), no one can calculate the real identity of the vehicle i through the pseudo-identity pair. Also, because each signature uses a different pseudonymous pair (AID_i^1, AID_i^2). Therefore, personal privacy is protected.

3) THE RESIST REPLAY ATTACKS

Because of the characteristics of wireless communication, the information we sent is often easy to be captured. Although attackers cannot forge signatures to tamper with information and forge information attacks, they can replay attacks. For example, suppose the vehicle i is found to have a traffic accident in a certain section of the road, in order to make the traffic control center deal with the incident and reasonably clear the road. The vehicle i sent a message M_i at time T_1, and both the attacker and the traffic center obtained M_i. The transportation center went through a series of certification processes to make sure that it was credible, so it was reasonably arranged. If the attacker uses the obtained information to send out the message M_i again at time T_2, the traffic center will still pass the certification and take measures. However, it takes manpower and resources to find out that this is a hoax, and the traffic arrangement for emergencies will make the traffic situation chaotic. Imagine if there were an infinite number of such messages, and the whole system crashed.

In our scheme, we used private key timestamp signatures for individual authentication to prevent replay attacks. In batch authentication, we asked V_T to collect the information by verifying the timestamp of each information, consolidating the information that is not in question, and then V_T signs the time with its own group key and sends the consolidated information to the RSU. In intra-group authentication, we used the intra-group communication key to sign the timestamp and put it into the sending message.

Therefore, our scheme successfully withstands replay attacks in communication.

4) THE TRACEABILITY BY THE CA

In our scheme, in order to protect user privacy, we signed messages with different pseudonyms. As the only credible agency, CA can use the following formula to calculate the true identity of the vehicle. $AID_i^2 \bigoplus H(d_i^1 AID_i^1) = RID_i \bigoplus H(NP_{pub_i^1}) \bigoplus H(d_i^1 NP_{pub_i^1}) = RID_i$.

Part of the private key d_i^1 of vehicle i is only known by CA, so other vehicles and RSU cannot calculate the real identity of the vehicle. When a vehicle i delivers false messages and conducts illegal operations, the RSU can report to the CA, which calculates to obtain its real identity. This satisfies the traceability of the real identity of the vehicle.

VI. PERFORMANCE EVALUATION

In this section, we will evaluated the performance of the HPBS scheme primarily by verifying latency and transport overhead, and compare it with the related schemes, such as ECDSA [40] and LIAP [41] in terms of computation and transmission overheads. Considered that the ECDSA scheme is the signature algorithm adopted by IEEE1609.2 standard, we adopted it as a comparison scheme. LIAP is A local identity-based anonymous message authentication protocol. Our scheme has the same points as LIAP: (1) We both used a hybrid approach to design anonymous message authentication schemes; (2) We used identity-based and PKI-based to design mixed schemes. Differences between our approach and LIAP:(1) LIAP uses anonymous message authentication in part. Our scheme utilizes PKI-based ideas locally; (2) Our scheme introduces proxy vehicles. Therefore, we used LIAP as our comparison object. Here, we only considered the communication overhead of V2V and V2I, and we do not analyze the communication between CA and RSU.

TABLE 3. Comparisons of the speed of three signature schemes (ms).

Scheme	Verify a single message	Verify n messages
ECDSA	$4T_{mul}$	$4nT_{mul}$
LIAP	$T_{mul}+T_{mtp}+3T_{par}$	$(n+1)T_{mul}+nT_{mtp}+3T_{par}$
HPBS	$2T_{mul}+2T_{mtp}+6T_{par}$	$(m+n/m)T_{mul}+(m+n/m)T_{mtp}+6T_{par}$,m is the number of the proxy vehicles

A. COMPUTATION OVERHEAD ANALYSIS

In this section, we calculated the calculation cost of vehicle vehicle validation general vehicle information and RSU vehicle integration information respectively. Here, we added the two as total message validation computation overhead and compare the computation overhead with the other two scenarios in detail.

In the V2I communication phase, The computational overhead is mainly generated by message validation. The operations required to validate the message are as follows. T_{mul} represents the time required to perform a point multiplication, T_{mtp} represents the time required to perform a MapToPoint hash operation, and T_{par} represents the time required to perform a pairing operation. The experiments run on an Intel i7-9750 3 GHZ machine. According to [28], The following parameters are obtained: T_{mul} is 0.39 ms, T_{mtp} is 0.09 ms and T_{par} is 4.5 ms.

TABLE 3 shows a comparison of three schemes for the computational overhead of an RSU signed for a single message and n messages. The time required for the ECDSA scheme to validate a message is $4T_{mul}$, and the time required for the validation of n messages is $4nT_{mul}$. The LIAP scheme takes $T_{mul}+T_{mtp}+3T_{par}$ to validate a message and $(n+1)T_{mul}+nT_{mtp}+3T_{par}$ to validate n messages.

First, we assumed that the traffic density of the vehicle is equal to the number of messages to be verified sent by the vehicle during the cycle, and each vehicle sends a message at a fixed time of 300ms as the cycle. We assumed that in the RSU communication range, the number of proxy vehicles is m and the number of messages to verify is n. Therefore, the average number of messages that need to be validated per agent vehicle is $\lceil \frac{n}{m} \rceil$. The time it takes to validate a message with our scheme is $2T_{mul}+2T_{mtp}+6T_{par}$, and the time it takes to validate n messages is $(m+n/m)$ $T_{mul}+(m+n/m)T_{mtp}+6T_{par}$.

FIGURE 4 illustrates the relationship between the number of messages and the number of proxy vehicles within an RSU's coverage area and the computation overhead of the RSU. We can see from the figure that the computation overhead increases as the number of messages and the number proxy vehicles increases. When the number of proxy vehicles is greater than 1, the calculation cost of our scheme is much higher than that of the other two schemes. Below, we drew the comparison line diagram of the three schemes of proxy vehicles $m=2$ and $m=3$.

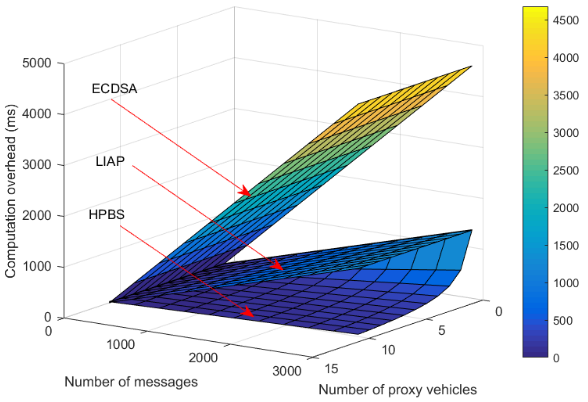


FIGURE 4. Computation overhead *vs*. Number of messages and Number of proxy vehicles.

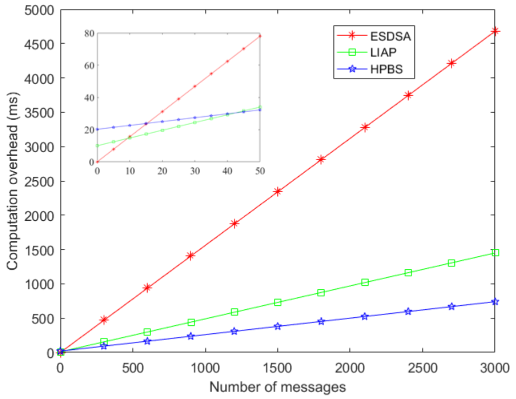


FIGURE 5. Computation overhead *vs*. Number of messages, the number proxy vehicles $m=2$.

FIGURE 5 shows the change of the computational overhead of the three schemes with the increase of the number of messages when the number of proxy vehicles in the RSU communication range is 2. From the figure, we can see that our scheme requires less computational overhead than the other two schemes when the number of messages is more than 50. At the same time, as the number of messages increases, the computational overhead of our scheme is smaller than that of the other two schemes.

From FIGURE 6, We can saw that when there are three proxy vehicles in the communication range of RSU, the calculation cost of our scheme is less than the other two schemes as the number of messages increases. By comparing FIGURE 5 and FIGURE 6, we can find that as the number of proxy vehicles in the RSU communication range increases, the delay required to validate messages will decrease.

In V2V communication phase, The message authentication between vehicles is mainly divided into two ways: one is the authentication of vehicles within a group, and the other is the authentication of vehicles between different groups. Message authentication between vehicles in the same group only requires the computational overhead of decrypting a

TABLE 4. Comparisons of transmission overhead of three schemes (byte).

Scheme	A single message	n messages
ECDSA	$42 + 125$ bytes	$42n + 125n$ bytes
LIAP	92 bytes	$92n$ bytes
HPBS	$21 + 42 + 21 + 42$ bytes	$21 + 42n + 21 + 42m$ bytes, m is the number of the proxy vehicles

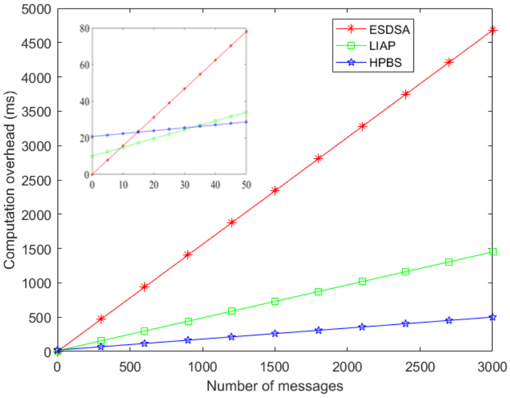


FIGURE 6. Computation overhead *vs*. Number of messages, the number proxy vehicles $m = 3$.

symmetric signature using the group key. The computational overhead required for message authentication between vehicles that are not in the same group is a bilinear authentication operation, and the computational overhead required is $T_{mul} + T_{mtp} + 3T_{par}$.

B. TRANSMISSION OVERHEAD ANALYSIS

In this section, We analyzed and compared the transmission overhead of ECDSA, LIAP, and HPBS. In our scheme, the transport overhead we calculate includes the transport overhead from the normal vehicle to the proxy vehicle and the transport overhead from the proxy vehicle to the RSU.

TABLE 4 shows the number of bytes that need to be transferred under one message and n messages for each of the three scenarios. Here, we do not count message M_i as transport overhead. Based on the authentication process in section IV, we can calculate that the number of bytes of message (AID_i, σ_i) transmitted from the ordinary vehicle to the proxy vehicle is 21+42n. The information transferred from the proxy vehicle to the RSU is (AID_T, σ_T), and we can calculate that the transfer overhead is 21+42m. And m is the number of proxy vehicles. We can figure out that the total cost of the transfer is $21 + 42n + 21 + 42m$.

FIGURE 7 illustrates the relationship between the number of messages and the number of proxy vehicles within an RSU's coverage area and the transmission overhead of the RSU. From the picture, we can see that, with the increase of the number of messages, the number of transmitted bytes of the three schemes all shows an increasing trend. The transmission overheads of ECDSA is the largest among the three schemes, and the transmission overhead of the HPBS is much smaller than the other two.

From FIGURE 8, we can clearly saw the comparison of transmission overhead of the three schemes when there are two proxy vehicles in the communication range of the RSU.

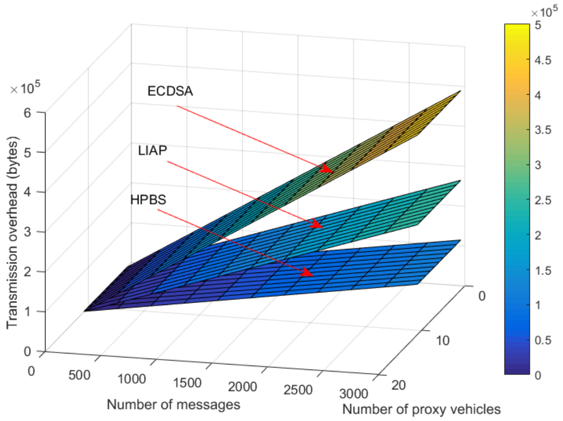


FIGURE 7. Transmission overhead *vs*. Number of messages and Number of proxy vehicle.

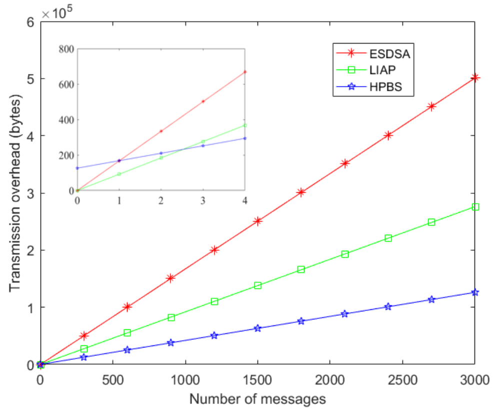


FIGURE 8. Transmission overhead *vs*. Number of messages, the number proxy vehicles $m = 2$.

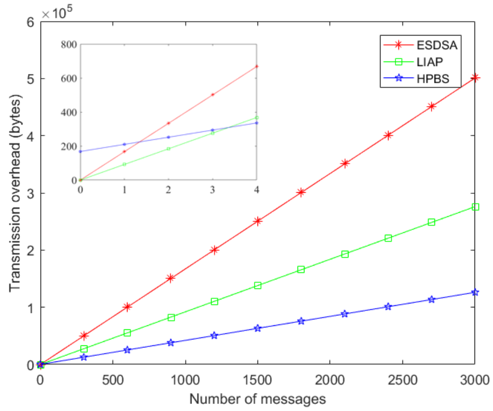


FIGURE 9. Transmission overhead *vs*. Number of messages, the number proxy vehicles $m = 3$.

We found that after the number of messages is greater than 3, our scheme has the lowest transmission cost among the three schemes and the gap between the three becomes larger as the number of messages increases.

By comparing FIGURE 9 and FIGURE 8, we can found that the transmission overhead of our scheme decreases slightly as the number of proxy vehicles increases. By looking at the number of proxy vehicles, there was a slight increase in the transmission overhead of our scheme. However, the transmission overhead of our scheme is always much less than that of the other two schemes.

VII. CONCLUSION

In HPBS, we used the computing power of the proxy vehicle to reduce the burden on the RSU, where the proxy vehicle can batch authenticate messages from other vehicles and the RSU is responsible for authenticating messages from the agent vehicle. At the same time, we use the group keys jointly generated by the proxy vehicle and the RSU to make intra-group V2V communication more efficient. In the event of an illegal operation of a node, HPBS can trace the node through CA and obtain its true identity. In addition, HPBS is able to withstand replay attacks. HPBS was analyzed and compared with other schemes in terms of computational and transmission overhead.

In the work of HPBS, we mainly proposed a hypothetical password algorithm that takes buses and other similar vehicles as proxy vehicles. Since the route of these special vehicles is fixed and concentrated on the road with high traffic flow, it is more advantageous for the scheme to be applied in practice. In the future, we will used the trust extension to increase the number of agent vehicles, which will further improve the efficiency of certification. In addition, we will also use game theory to study the incentive mechanism to minimize redundant authentication events.

REFERENCES

[1] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Anonymity analysis on social spot based pseudonym changing for location privacy in VANETs," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[2] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

[3] M. Arshad, Z. Ullah, N. Ahmad, M. Khalid, H. Criuckshank, and Y. Cao, "A survey of local/cooperative-based malicious information detection techniques in VANETs," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, p. 62, Dec. 2018.

[4] Z. Ning, J. Huang, and X. Wang, "Vehicular fog computing: Enabling real-time traffic management for smart cities," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 87–93, Feb. 2019.

[5] X. Wang, Z. Ning, M. Zhou, X. Hu, L. Wang, B. Hu, R. Y. K. Kwok, and Y. Guo, "A privacy-preserving message forwarding framework for opportunistic cloud of things," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 5281–5295, Dec. 2018.

[6] X. Wang, Z. Ning, and L. Wang, "Offloading in Internet of vehicles: A fog-enabled real-time traffic management system," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4568–4578, Oct. 2018.

[7] A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Vehicular ad hoc networks: A new challenge for localization-based systems," *Comput. Commun.*, vol. 31, no. 12, pp. 2838–2849, Jul. 2008.

[8] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[9] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 57, no. 6, pp. 3357–3368, Nov. 2008.

[10] D. He, C. Chen, S. Chan, and J. Bu, "Analysis and improvement of a secure and efficient handover authentication for wireless networks," *IEEE Commun. Lett.*, vol. 16, no. 8, pp. 1270–1273, Aug. 2012.

[11] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1606–1617, May 2010.

[12] A. Wasef and X. Shen, "Efficient group signature scheme supporting batch verification for securing vehicular networks," in *Proc. IEEE Int. Conf. Commun.*, Cape Town, South Africa, May 2010, pp. 1–5.

[13] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. IEEE INFOCOM 27th Conf. Comput. Commun.*, Phoenix, AZ, USA, Apr. 2008, pp. 246–250.

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

[15] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Securiry*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.

[16] J. Zhang, Z. Sun, S. Liu, and P. Liu, in *Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage*, Nov. 2016, pp. 145–155.

[17] L. Yao, C. Lin, G. Wu, T. Jung, and K. Yim, "An anonymous authentication scheme in data-link layer for VANETs," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 22, no. 1, pp. 1–13, May 2016.

[18] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 8, pp. 2193–2204, Aug. 2016.

[19] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," *Commun. ACM*, vol. 28, no. 10, pp. 1030–1044, Oct. 1985.

[20] C.-I. Fan, R.-H. Hsu, and C.-H. Tseng, "Pairing-based message authentication scheme with privacy protection in vehicular ad hoc networks," in *Proc. Int. Conf. Mobile Technol., Appl., Syst. Mobility*, Sep. 2008, pp. 1–7.

[21] X. Yue, B. Chen, X. Wang, Y. Duan, M. Gao, and Y. He, "An efficient and secure anonymous authentication scheme for VANETs based on the framework of group signatures," *IEEE Access*, vol. 6, pp. 62584–62600, Oct. 2018.

[22] J. Zhang, H. Zhong, J. Cui, Y. Xu, and L. Liu, "An extensible and effective anonymous batch authentication scheme for smart vehicular networks," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3462–3473, Apr. 2020.

[23] X. Li, Y. Liu, and X. Yin, "An anonymous conditional privacy-preserving authentication scheme for VANETs," in *Proc. IEEE 21st Int. Conf. High Perform. Comput. Commun. IEEE 17th Int. Conf. Smart City IEEE 5th Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Zhangjiajie, China, Aug. 2019, pp. 1763–1770.

[24] H. Hasrouny, C. Bassil, A. E. Samhat, and A. Laouiti, "Group-based authentication in V2V communications," in *Proc. 5th Int. Conf. Digit. Inf. Commun. Technol. Appl. (DICTAP)*, Beirut, Lebanon, Apr. 2015, pp. 173–177.

[25] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1711–1720, Mar. 2016.

[26] T. Gao, X. Deng, Q. Li, M. Collotta, and I. You, "APPAS: A privacy-preserving authentication scheme based on pseudonym ring in VSNs," *IEEE Access*, vol. 7, pp. 69936–69946, Mar. 2019.

[27] Z. Liu, L. Xiong, T. Peng, D. T. Peng, and H. B. Liang, "A realistic distributed conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Access*, vol. 6, pp. 26307–26317, May 2018.

[28] M. S. I. Mamun and A. Miyaji, "An optimized signature verification system for vehicle ad hoc NETwork," in *Proc. 8th Int. Conf. Wireless Commun., Netw. Mobile Comput.*, Shanghai, China, Sep. 2012, pp. 1–8.

[29] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[30] L. Zhang, Q. Wu, B. Qin, and J. Domingo-Ferrer, "APPA: Aggregate privacy-preserving authentication in vehicular ad hoc networks," in *Proc. Int. Conf. Informat. Secur.*, 2011, pp. 293–308.

[31] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. Annu. Int. Cryptol. Conf.*, 2001, pp. 213–229.

[32] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. 84, no. 5, pp. 1234–1243, May 2001.

[33] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *J. Cryptol.*, vol. 17, no. 4, pp. 297–319, Jul. 2004.

[34] K. Ren, W. Lou, K. Kim, and R. Deng, "A novel privacy preserving authentication and access control scheme for pervasive computing environments," *IEEE Trans. Veh. Technol.*, vol. 55, no. 4, pp. 1373–1384, Jul. 2006.

[35] K. Sampigethava, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," in *Proc. Int. Workshop Veh. Ad Hoc Netw.*, 2006, pp. 1–15.

[36] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.

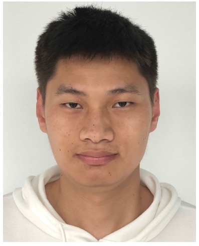
[37] V. S. Miller, "Use of elliptic curves in cryptography," in *Proc. Conf. Theory Appl. Cryptograph. Techn.*, 1985, pp. 417–426.

[38] *Dedicated Short Range Communications (DSRC)*. Accessed: Jun. 16, 2011. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5888501.html

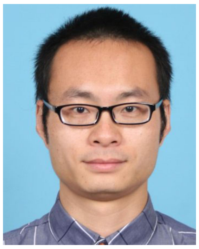
[39] M. Burrows, M. Abadiand, and R. Needham, "A logic of authentication," *ACM Trans. Comput. System.*, vol. 8, no. 1, pp. 18–36, Feb. 1990.

[40] *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management*, IEEE Standard 1609.2, 2006.

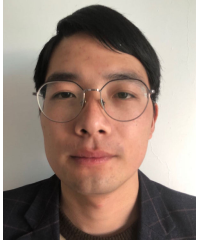
[41] S. Wang and N. Yao, "LIAP: A local identity-based anonymous message authentication protocol in VANETs," *Comput. Commun.*, vol. 112, pp. 154–164, Nov. 2017.



HUA LIU is currently pursuing the master's degree with the Zhejiang University of Science and Technology. His research interests wireless mesh network security, cryptography, and information theory.



HAIJIANG WANG received the M.S. degree from Zhengzhou University, in 2013, and the Ph.D. degree from Shanghai Jiao Tong University, in 2018. He is currently a Teacher with the School of Information and Electronic Engineering, Zhejiang University of Science and Technology. His research interests include cryptography and information security, in particular, public key encryption, attribute-based encryption, searchable encryption.



HUIXIAN GU is currently pursuing the master's degree with the Zhejiang University of Science and Technology. His research interests edge cache, wireless communication, and information theory.