# A Blockchain-based Privacy-Preserving Authentication Scheme with Anonymous Identity in Vehicular Networks

Liang Wang, Dong Zheng, Rui Guo, ChenCheng Hu, and ChunMing Jing
*(Corresponding author: Liang Wang)*

National Engineering Laboratory for Wireless Security
School of Cyberspace Security, Xi'an University of Posts and Telecommunications
Xi'an 710121, China
(Email: wangliang_zjk@163.com)

*(Received May 5, 2019; Revised and Accepted Dec. 12, 2019; First Online Feb. 1, 2020)*

## Abstract

With the rapid development of mobile network technology, Vehicular ad-hoc Networks (VANETs), one of the most promising applications in the smart transportation systems, have drawn widespread attention. Unfortunately, authentication and privacy protection of users have seriously restricted the development of VANETs. The past works used to allow a centralized trusted authority to distribute identity information and maintain the operation of the whole system lacking of distributed and decentralized security. In this paper, we propose an authentication scheme based on consortium blockchain with anonymous identity in VANETs. First, when authenticating and providing services, our scheme allows the vehicles using Pseudo IDs obtained from the Road Side Unit (RSU) to protect the privacy of the vehicles preventing location tracking due to disclosure of information. Second, based on consortium blockchain technology, it provides a decentralized, secure and reliable database for storing certificates and the pointer to storage location, which is maintained by the multiple Trusted Authorities (TAs) and RSUs. Furthermore, in the revocation, the RSUs are able to determine promptly that the vehicle has been revoked by adding a revocation tag to the pseudo ID instead of searching the entire certificate revocation list (CRL). According to the security and performance analysis, our scheme owns higher security and efficiency.

*Keywords: Anonymity; Blockchain; Privacy-preserving; Revocation; Vehicular Ad-Hoc Networks (VANETs)*

## 1 Introduction

Recently, with the rapid development of the automobile industry and Internet of Things (IOT), Vehicular ad-hoc Networks (VANETs) have become one of the hotspots in the research fields of intelligent transportation systems for scholars focusing on how to improve the efficiency and safety of the road [5, 11, 23, 25]. It is estimated that the number of registered vehicles around the world wil reach 2 billion within the next 10 to 20 years [4]. Based on the On-Board-Unit(OBU) installed on vehicle, VANETs include two types of communications:

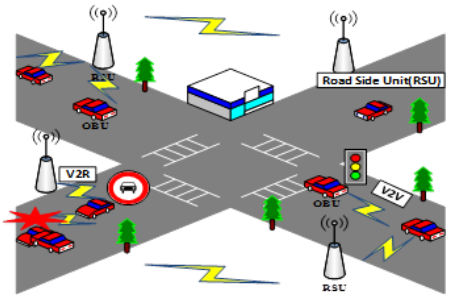


Figure 1: The architecture of VANETs

1) The Vehicle-to-Vehicle (V2V);

2) The Vehicle-to-Road Side Unit (V2R). The architecture of VANETs is shown in Figure 1. With the help of Road Side Units (RSUs), nearby vehicles can exchange traffic, weather and other information via the dedicated short range communication (DSRC) [10], which helps drivers make timely and reasonable driving strategies. In such situations, authentication and security need to be ensured.

However, due to the high mobility and variability of network topology, the system is vulnerable to be threaten by the malicious adversary in the VANETs. Therefore, security, privacy and authentication should be taken into account [2]. Specially, two types of issues, namely disclosure of location privacy and identity privacy pose some serious threats to the entire networks. Firstly, if the adversary

learns the location of a particular node, the node's communication behavior will be tracked and eavesdropped. In other words, an attacker can track the driving line of a user with a special identity. Secondly, it is extremely serious that malicious attackers launch a Sybil Attack by using these identity information stored in cloud servers. In order to provide secure communication environments, researchers used to focus on the traditional infrastructure, namely the public key infrastructure (PKI). Asymmetric cryptography algorithm and digital certificates are utilized in PKI, protecting identity information of the users via a centralized trusted third party (TA) [17]. However, with the number of vehicles increasing, the management of PKI certificates requires huge storage and computational overhead, especially for certificate revocation. Moreover, a single centralized trusted third party may cause a single point of failure. Therefore, how to provide an effective solution is still a problem remained to be solved urgently, such as efficiency and distributed security.

With all this in mind, blockchain is considered as a revolutionary technology to cope with the problems above. As the underlying technology of the Bitcoin, blockchain was initially proposed by Nakamoto in 2008 [16]. It utilizes a distributed database in the peer to peer (P2P) network to record all transaction behaviors and maintain a consistent and tamper-proof ledger. Due to high security and reliability, the combination of blockchain and VANETs has received considerable attention [21, 26]. On the one hand, in VANETs, all activities and information could be written into the immutable and unforgeable ledger, which can be verified and traced by all legitimate members. On the other hand, it can avoid single point of failure in a distributed way and enhance the security of the system.

## 1.1 Related Research

Compared with open access environment, providing a secure and reliable communication environment for vehicles plays an extremely important role in VANETs [3,27]. Therefore, authentication, privacy, and confidentiality of information should be taken into account seriously. Lin *et al.* [13] proposed a secure protocol based on group signature, which can guarantee privacy of users and provide the desired traceability for each vehicle. However, the pure group signature verification is usually time-consuming, and it is hard to meet the real-time requirements of the application in VANETs. For obtaining high privacy and security, Yao *et al.* [22] proposed a biometrics-based authentication scheme, which uses a temporary MAC address to conceal the real MAC address. Jiang *et al.* [6] adopt pseudonyms to realize batch authentication by using an identity-based signature (IBS). However, most of them are based on traditional digital signature technology of PKI, which have high computational and storage overhead. Vijayakumar *et al.* [20] proposed a secure authentication and key management mechanism to ensure the security of user's key in VANETs. Lim *et al.* [12] proposed an efficient protocol for fast dissemination of authentication messages, and Tan *et al.* [19] proposed a secure certificateless authentication to realize vehicle's identity authentication. However, these solutions rely on a centralized trusted third party and cannot provide the distributed security.

With the properties of decentralization, transparency, traceability and non-tampering, blockchain, a distributed public ledger shared and maintained by all nodes in the system, has attracted wide attention, not only in the financial industry but also in VANETs. Specifically, many researchers in VANETs focus on improving efficiency and security to ensure vehicle's privacy through blockchain technology. Yuan *et al.* [24] proposed a seven-layer conceptual model for Intelligent Transportation Systems (ITS) via blockchain technology, and claimed that the decentralized model will be the future of ITS. Dorri *et al.* [1] proposed a blockchain-based architecture to increase the security and protect the privacy of users. Although the privacy and security were considered in the paper, they do not give the concrete and practical scheme. Lei *et al.* [9] proposed a secure blockchain-based key management framework with a security managers (SMs) in ITS. Lu *et al.* [14] designed a decentralized anonymous reputation system using blockchain technology for VANETs. Rowan *et al.* [18] proposed a blockchain-based PKI and an inter-vehicle session key establishment protocol for secure V2V communications. In the above researches, the blockchain is applied to enhance security between information and energy interactions. However, these schemes are only suitable in Bitcoin. Malik *et al.* [15] proposed an authentication and revocation of framework using blockchain technology, which authenticates vehicles in a decentralized way. However, they store a certain number of bytes using the OP_RETURN instruction in Bitcoin. Actually, storing a large amount of non-transaction information in the Bitcoin network affects the performance of system, therefore, the size of OP_RETURN instruction is limited, and with the number of vehicles increasing, the amount of information stored in the blockchain will be enormous, which directly affects the scalability of the system.

## 1.2 Our Contributions

In this paper, we propose an anonymous authentication scheme based on consortium blockchain in VANETs, and the real identity of the vehicle can be concealed by using pseudo IDs to ensure the privacy of the vehicle. Specifically, we make the following contributions:

1) Our scheme allows the vehicles using Pseudo IDs obtained from the Road Side Units (RSUs) to conceal the real identity of the vehicle, which can prevent location tracking. Furthermore, each transaction includes a unique transaction ID (TID) and the RSU can quickly verify vehicular identity information using TIDs.

2) Based on consortium blockchain, we conduct a rigorous review of the nodes joining the system to ensure the confidentiality of the ledger and provide a decentralized, distributed, reliable database maintained by multiple trusted authorities (TAs) and RSUs for storing certificates. In addition, a great deal of anonymous certificates are stored in the trusted cloud server and pointers to the storage location are stored in the blockchain, which can improve the scalability of the system.

3) In the revocation, compared with searching the entire certificate revocation list (CRL), RSUs are able to determine promptly that the vehicle has been revoked by adding a revocation tag in our scheme, and the latter requires less computational overhead.

### 1.3 Organization

The remainder of this paper is as follows: Section 2 demonstrates a succinct concise overview of the consortium blockchain, VANETs and assumptions. In Section 3, the system model of anonymous authentication based on consortium blockchain for VANETS is discussed. In Section 4, the proposed scheme including registration, authentication and revocation is given. Section 5 analyzes the security of our scheme and evaluates the theoretical performance. Finally, Section 6 concludes the paper.

## 2 Preliminaries

### 2.1 Consortium Blockchain

The Consortium blockchain, a type of permission blockchain, is not completely decentralized, but it is a multicenter blockchain as shown in Figure 2. The predefined authoritative node A can select the accounting nodes 1, 2 and 3 by voting and the remaining nodes are the ordinary nodes. Compared with public blockchain, only legitimate nodes (member nodes) can access the ledger and view related information stored in consortium blockchain by setting up access permissions. In addition, the access authority and record authority of the ledger are determined jointly by authoritative nodes to ensure the confidentiality of ledger, and provide a higher security. Generally, considering the efficiency of the system, it do not use mining mechanisms, such as Proof of Work (POW) algorithm.

### 2.2 VANETs

VANETs, a special wireless ad-hoc network, can provide a secure and efficient environment for Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Infrastructure (V2I) communication as shown in Figure 1. There are three types of entities in VANETs: Trusted Authority (TA), Roadside Unit (RSU), and On-Board Unit (OBU).

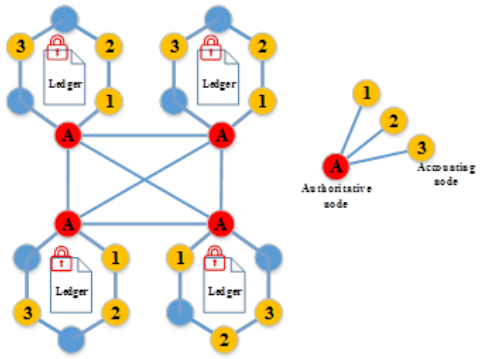


Figure 2: Structure of consortium blockchain

TA plays an extremely important role in the process of vehicle registration and authentication. Multitude of wireless gateway points, *i.e.*, RSUs, are deployed along the roadside. Through the RSU, Vehicles can share valuable driving information with neighboring vehicles to improve traffic efficiency and safety. OBU configured into vehicle is responsible for communicating with RSU by utilizing dedicated short range communication (DSRC) radio.

### 2.3 Assumption

The process of registration is divided into two phases. Firstly, the vehicle obtains the public key certificate from the $TA$. Secondly, it obtains the Pseudo ID from the RSU within the region covered by the $TA$. In addition, the distance affects the communication delay, therefore, the nearest RSU to the vehicle is responsible for generating $PID$ in our scheme. All of the above are prerequisites for authentication, we need make the following assumptions:

1) We assume that TAs and RSUs generated Pseudo ID for vehicle are completely trusted and they are not be compromised.

2) When the vehicle obtains the public key certificate from the nearest TA, the locations of RSUs within the region covered by the TA are stored in the OBU installed in the vehicle. Therefore, at any time, the vehicle knows the nearest RSU and the RSU generates pseudo ID for vehicles quickly.

3) we assume that the cloud server in our work is absolutely trustworthy.

## 3 System Model

In this section, we introduce the system model and the specific function of each entity in the system model.

There are five entities in the proposed system: A Traffic Department (TD) , multiple Trust Authorities (TAs), Road Side Units (RSUs), On Board Units (OBUs) installed in vehicle and a Trusted Cloud Server (TCS). It is worth noting that TD, TA and RSU represent three types

of nodes, namely supervisory nodes, accounting nodes (revocation nodes) and verification nodes. As shown in Figure 3.

- Traffic Department: Firstly, as the supervisory node of the system, the traffic department is responsible for supervising the operation of the entire system. Secondly, the supervisory node needs to select the accounting nodes (TAs) in advance for generating the transaction information and uploading them to the blockchain. In addition, the vehicle needs to submit personal information to the TD before registration and obtain a unique plate number namely VID;

- Trust Authority: There are multiple authoritative nodes in our system and their accounting rights are granted by the TD. There are mainly three functions for TA. First, it is responsible for assigning a public-private key pair to the vehicle and RSU within the region coverd by the TA, which are used to authenticate between vehicle and RSU. Second, a candidate transaction set is generated by the TA including a large number of public key certificates encrypted using the public key of the TA. Finally, the TA uploads the integral transactions to the blockchain. It is worth noting that a integral transaction consists of a candidate transaction and a pointer to the storage location of pseudo ID;

- Road Side Unit: There are many RSUs distributed within the region covered by each TA. Each RSU is a verification node in the blockchain and is mainly responsible for generating a pseudo ID for the vehicles and sending the generated pseudo ID to the TCS. In addition, a pointer to the storage location of pseudo ID is transferred to the TA. RSU1 and RSU2 represent two different RSUs;

- On Board Unit: Due to the limited resources and computing power of OBU, it only participates in the simple encryption and transmission of data, and sends the collected data as a data set to the RSU;

- Trusted Cloud Server: We can only upload the user's real identity and the hash index of the pseudo ID to the blockchain, and a large number of pseudo IDs are sent to a Trusted cloud server. Here, we assume that this cloud server is absolutely trustworthy.

# 4 The Proposed Anonymous Authentication Scheme in VANETs

In this section, we describe the blockchain-based anonymous authentication scheme in detail including system initialization, registration, mutual authentication and expeditious revocation.

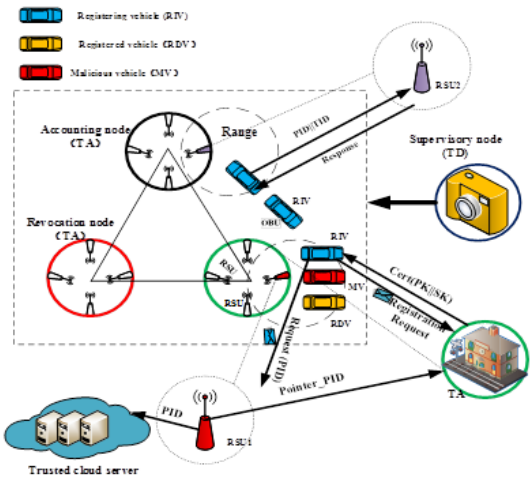


Figure 3: System model

## 4.1 System Initialization

The notations used in this paper are given in Table 1.

Table 1: Notations

| Notation | Meaning |
|---|---|
| $P_{V_i}$ | The public key of vehicle |
| $SK_{V_i}$ | The private key of vehicle |
| $P_{R_i}$ | The public key of $i^{th}$ RSU |
| $TX_i()$ | Candidate transaction set |
| $T_i()$ | Timestamp |
| $TID_j()$ | Transaction ID of $j^{th}$ transaction |
| $POINTER$ | A pointer to the storage location of Pseudo ID |
| $E()$ | Encrypt |
| $Sig()$ | Digital signature |
| $R$ | Random numbers |

The system is comprised of five participants: Traffic Department (TD), multiple Trust Authorities $TA = \{TA_1, TA_2, ..., TA_n\}$, vehicle sets $V = (V_1, V_2, ..., V_i)$, Roadside Units $R = \{RSU_1, RSU_2, ..., RSU_i\}$ and Trusted Cloud Server. In the registration, different participants prepare to be occupied with numerous domain parameters required for security operations. The system is maintained by multiple Trust Authorities for Elliptic curve cryptography (ECC) based PKI technology, and system parameters set $\{q, a, b, P\}$ is initialized. Here, $a$ and $b$ are constants defining the Elliptic curve equation ($a, b \in F_q$ and $4a^3 + 27b^2 \neq 0$). $P$ is the generator of the Elliptic Curve $E$ with prime order q. There are many RSUs within coverage of each TA. We assume that $TA_1 \in TA$ needs to distribute ECC public-private key pairs to the RSUs. $TA_1$, one of multiple trusted authorities, selects a integer set $(a_1, a_2, ..., a_n \in Z_q)$ as private keys of RSUs and generates a public key set $(P_{R1}, P_{R2}, ..., P_{Rn})$, where $P_{Rn} = a_i \cdot P$.

The consortium blockchain is established amoung TD, multiple Trust Authorities and RSUs. Multiple Trust Authorities are responsible for generating new identities for vehicles. The $TA_1$ elected as a accounting node by using suitable voting mechanism uploads transaction information to the blockchain.

## 4.2 Registration of the Vehicle

In our work, there are two stages for the vehicle to complete the registration. Firstly, the TA is responsible for generating an ECC public-private key pair namely $P_{V_i}$ and $SK_{V_i}$ for the vehicle, and generating a candidate transaction set waiting for being uploaded. Secondly, the RSU generates a pseudo ID for the vehicle.

1) The TA generates a Public-Private key pairs for $V_i$:

Table 2: Registration of the vehicle

| |
|---|
| $1.V_i \rightarrow TA_1 :< VID_i \| \| Other >$ |
| $2.TA_1 \rightarrow VID_i :< Verify(VID_i) >$ |
| $3.TA_1 \rightarrow V_i :< d \| \| P_{V_i} \| \| Sig\{H(P_{V_i} \| \| d)\} \| \| T_1 >$ |
| $4.TA_1 \rightarrow V_i :$ $< TX_i\{E(Cert_{V_i})\} \| \| TX_{i+1}\{E(Cert_{V_{i+1}})\} >$ |

The steps of registration are described in Table 2. The vehicles register with TA for the first time by submitting their $VID_i$ issued by $TD$. The supervisory node ($TD$) in the system need to select a node being responsible for the registration of the vehicle according to a specific consensus algorithm. Here, we assume that $TA_1$ is only an authoritative node that is temporarily elected for this registration.

$TA_1$ verifies the $VID_i$ and selects a integer $b \in Z_q$ as the private key of the vehicle namely $SK_{v_i} = b$ and generates a public key $P_{V_i}$, where $P_{V_i} = b \cdot P$. $TA_1$ send $< b, P_{V_i}, H(Sig), Sig, T_1 >$ to the vehicle through a secure channel, and at the same time, it generates a partial transaction set waiting for being uploaded including real identities of a large number of vehicles.

It is worth noting that the public key certificates are stored in the partial transaction set in the form of ciphertext, and they are encrypted with the public key of the $TA_1$.

2) The RSU generates a Pseudo ID for $V_i$:

The vehicle sends a request message encrypted with public key of $RSU_1$ including the public key certificate $P_{V_i}$ obtained from the $TA_1$ and timestamp $T_1$. After receiving the request message, $RSU_1$ can select a random number $R_1 \in Z_q$ and calculate a message $M_1 = a \cdot P_{V_1} \cdot R_1$ for the vehicle. The vehicle selects a random number $R_2 \in Z_q$ and calculates two messages $M_2$, $M_3$, where $M_2 = b \cdot P_{R_1} \cdot R_1$ and $M_3 = R_2 \cdot M_1$. Here, $(P_{R_1}, a)$ is the public-private key pair of $RSU_1$. The vehicle sends a reply message $M = M_2 || M_3$ and a $T_1$ to $RSU_1$, and $RSU_1$ can verify the identity of the vehicle by determining if $M_3$ is equal to $M_4$, where $M_4 = M_2 \cdot R_2$. After the identity of the vehicle $V_i$ is authenticated, the RSU sends the pseudo ID with the timestamp $T_1$ to the vehicle and at the same time, the vehicle has completed registration.

**Algorithm 1** Generation of Pseudo ID

```
Begin
A vehicle V_i wants to send a Request to the nearby RSU_1.
Let Request =< E_{P_{R_1}}(Cert_{V_i}(P_{V_i})||T_1) >.
The RSU_1 receives the Request from V_i.
Let M_1 = a · P_{V_1} · R_1.
The RSU_1 sends to the M_1 to V_i.
The vehicle V_i sends to a Reply to the nearby RSU_1
Let M_3 = R_2 · M_1, and M_2 = b · P_{R_1} · R_1.
Let Reply = M_3||M_2.
The RSU_1 verifies the information of the vehicle V_i.
Let M_4 = M_2 · R_1.
if M_3 = M_4 then
    Let M = PID_i||T_1
    Send message M to the vehicle.
end if
Periodically refresh the PID_i
End
```

## 4.3 Uploading Transaction to Blockchain

After sending the pseudo ID to vehicle, the $RSU_1$ will send the $PID_i$ generated for this vehicle to the Trusted Cloud Server and forward a pointer to the memory address of $PID_i$ namely $POINTER\_PID_i$ to the $TA_1$.

The $TA_1$ records the pointer in the partial transaction previously waiting to be uploaded. At the same time, the $TA_1$ generates a complete transaction set and uploads it to the blockchain. In addition, we redefine contents of each transaction in blockchain, and each transaction includes a public key certificate encrypted by using public key of $T_1$, a pointer and a transaction ID as shown in Figure 4. The registration information of the vehicle forms a transaction with a uniquely identified transaction ID, namely $TID_j$. Using transaction ID, we can determine the identity of a vehicle by viewing records stored in the blockchain.

## 4.4 Mutual Authentication Between RSU2 and Vehicle

The vehicle $V_i$ leaves the region covered by $RSU_1$ and enters a region covered by $RSU_2$ as illustrated in Figure 5. It is critical for the vehicle and $RSU_2$ to complete

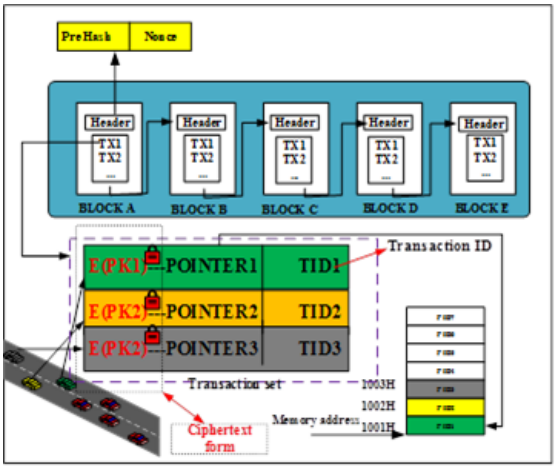


Figure 4: Transaction format of our scheme

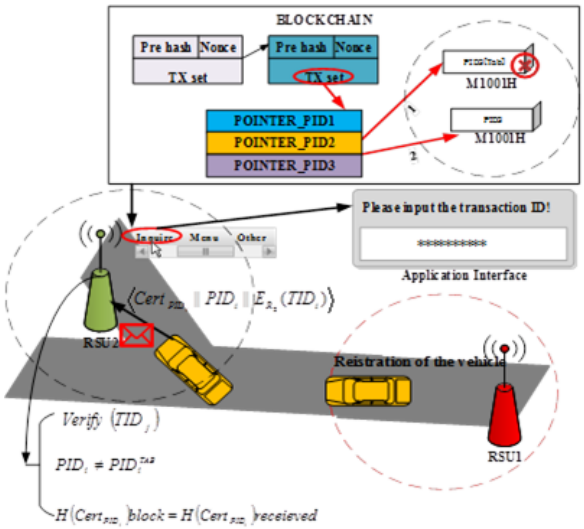


Figure 5: Mutual authentication between $RSU_2$ and vehicle

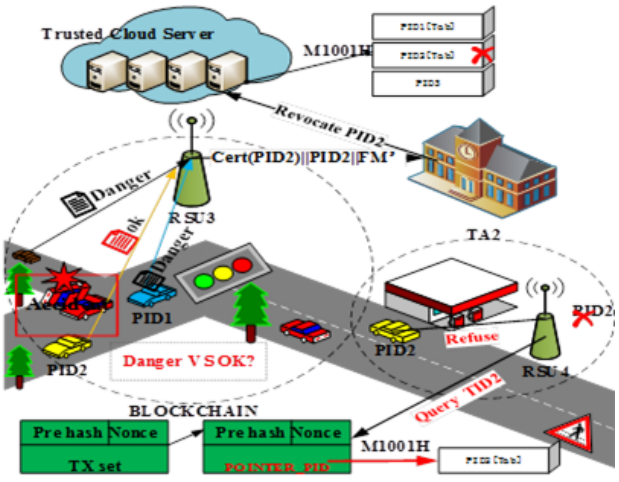


Figure 6: Revocation of malicious vehicle

anonymous authentication. The authentication process is divided into five steps:

- **Step 1:** The vehicle sends an authentication message $M_i$ including $PID_i$, $Cert_{PID_i}$, $H(Cert_{PID_i})$, a timestamp $T_2$ and a transaction ID encrypted with the public key of $RSU_2$ namely $E_{P_{R_2}} < TID_j >$ to $RSU_2$.
- **Step 2:** After receiving the message $M_i$, the $RSU_2$ decrypts the message $M_i$ by using its private key $a_2$ and gets the $PID_i$ transaction ID ($TID_j$), and timestamp $T_2$. The $RSU_2$ can verify the legality of the vehicle by querying the blockchain using $TID_j$.
- **Step 3:** Based on the transaction ID provided by the $TA_1$, the $RSU_2$ can quickly know identity information of the vehicle by visiting transaction information instead of traversing the entire blockchain system.
- **Step 4:** Firstly, through the transaction information recorded in the blockchain, the $RSU_2$ determines whether the transaction information corresponding to the $TID_j$ exists. If it does not exist, the vehicle can be considered as an illegal node. Secondly, if a pointer to $PID_i$ has a revocation tag namely $PID_i^{TAB}$, the information provided by the vehicle is invalid. Finally, $RSU_2$ can verify whether the message has been tampered with by comparing the $H(Cert_{PID_{receieved}})$ with $H(Cert_{PID_i})$. If the equation $H(Cert_{PID_i}) = H(Cert_{PID_{receieved}})$, the vehicle is legal.
- **Step 5:** Once the legality of vehicle identity is verified, $RSU_2$ can provide the corresponding service to it.

## 4.5 Expeditious Revocation

In the revocation, we assume that there are some reports: "Dangerous", "OK" and "dangerous" from three vehicles in the region covered by $RSU_3$ for the same road condition, and contents of the message are proven fallacious by using the evaluation algorithm. As shown in Figure 6, $PID_1$, $PID_2$, $PID_3$ represent three different vehicles respectively.

When the RSU finds that the $PID_2$ is sending "Forged Message" ("$FM$"), the RSU forwads a message including $Cert_{PID_2}$, $PID_2$ and "$FM$" to $TA_2$, and the message is encrypted by using the public key of $TA_2$. Once verified, the $TA_2$ sends a revocation command to the Trusted Cloud Server (TCS) through a secure channel. In our work, we set a revocation tab $PID_2^{TAB}$. The $TA_2$ is responsible for updating ledger in this paper. When the vehicle ($PID_2$) enters the region covered by the $RSU_4$, the $RSU_4$ can query the information stored in the blockchain and determine whether the vehicle has been revoked. Because of obtaining the $PID_2^{TAB}$ instead of the ($PID_2$), the system refuses to provide the corresponding service for vehicles.

The data stored in the blockchain is just a pointer to the storage location. When a malicious vehicle is found, the information of vehicle can be modified without changing the transaction itself. In addition, compared with searching the complete revocation list(CRL), we just need to determine whether the content of the pointer is $PID_i^{TAB}$ that requires lower computational overhead.

# 5 Security and Performance Analysis

## 5.1 Security Analysis

- **Confidentiality:** In the registration, the vehicle calculates message $M_1 = a \cdot P_{V_i} \cdot R_1$, where a is the private key of vehicle. $RSU_1$ calculates messages $M_2 = b \cdot P_{R_1} \cdot R_1$ and $M_3 = R_1 \cdot M_1$ , where $b$ is the private key of $RSU_1$. Two parties of the communication complete the mutual authentication by determining whether $M_2 \cdot R_1$ is equal to $R_2 \cdot M_1$. Messages encrypted with their public key can't be decoded, unless the attacker can obtain their private key. Specifically, the process of obtaining the private key is an ECDLP problem. Therefore, our scheme satisfies confidentiality.

- **Anonymity:** In the mutual authentication between the vehicle and the $RSU_2$, the vehicle sends a message $M$ including $PID_i$, $T_2$, $Cert_{PID_i}$ and $TID_i$ to the $RSU_2$, namely $< E_{P_{R_2}}(PID_i||Cert_{PID_i}||T_2||TID_i) >$. The $RSU_2$ decrypts it by using its private key, and determines whether the equation $H(Cert_{PID_i}) = H(Cert_{PID_{receieved}})$ is true by querying the information stored in the blockchain. In the authentication, the real identity of the vehicle can be concealed by using $PID_i$, which can ensure the anonymity of the vehicle.

- **Single point of failure:** There is no single point of failure in our scheme. Firstly, multiple Trusted Authorities (TAs) and RSUs jointly maintain a reliable ledger with authority. Each TA is responsible for distributing public-private key pairs for vehicles and RSUs. Secondly, in order to weaken permissions of the authoritative node TA, the RSU generates a pseudo ID for the vehicle in our scheme. Ultilizing a blockchain with authority can ensure distributed features. In addition, we have restricted on access to the ledger, so not all nodes can view the information stored in the blockchain.

- **Unforgeability:** Attackers generally complete authentication by forging the user's identity. We assume that the attacker forges the identity of the vehicle and calculates $M_2' = c \cdot P_{R_1} \cdot R_1$, where $c$ is the private key of attacker. In our work, the vehicle calculates message $M_2 = b \cdot P_{R_1} \cdot R_1$ and sends it to $RSU_1$. The equation $M_2'$ is not equal to $M_2$, unless the attacker can obtain the private key of the vehicle. The equation $M_2' \cdot R_1 \neq R_2 \cdot a \cdot P_{V_1} \cdot R_1$, the RSU failed to verify the identity of vehicle that the registration was unsuccessful.

- **Repaly attack:** The attacker achieves the purpose of deceiving the system by sending the same packets repeatedly. However, The process of authentication is based on random numbers $R1$, $R2$, and the random number can only be known by itself. It can ensure that there is no fixed connection for the request and reply between the vehicle and RSU, so the vehicle's private key cannot be decoded by the replay attack.

## 5.2 Performance Analysis

In this section, we analyze the feasibility of our scheme in terms of time consumption, storage capacity and security. The scalar multiplication operation on the Elliptic Curve, encryption operation, decryption operation and hash operation will be involved. In addition, it also involves digital signature and verifying. In our paper, we use the Elliptic Curves recommended by [7] and all operations are based on the ECC algorithm. Specially, we refer to the time of the scalar multiplication operation used in [8]. For the convenience of description, it will be defined in Table 3.

Table 3: The operation involved in this scheme

| Operation | Time |
|---|---|
| $T_{mul}$ | The time of a scalar multiplication operation |
| $T_{sig}$ | The time of one digital signature |
| $T_{Veri}$ | The time of verifying the signature |
| $T_H$ | The time of hash operation |
| $T_{enc}$ | The time of encryption operation |
| $T_{dec}$ | The time of decryption operation |

Specifically, our scheme involves digital signature, verifying, encryption operation, decryption operation and four scalar multiplication operations in the registration. The computation overhead of a vehicle can be summarized as: $4T_{mul} + 1T_{sig} + 1_{Veri} + 1T_{dec}$. There are multiple trusted authorities ($TAs$) in this paper. We assume that the maximum number of vehicles supported by a TA is 100 and n represents the number of vehicles. Under different values of n, the time consumption is tested in the registration and the authentication. As shown in Figure 7, in the registration, the total time taken for the 20 vehicles to complete the registration is 644.712ms. The number of vehicles increased from 20 to 100, and the total time taken is 3235.193 ms, which is the maximum time spent on registration.

In the authentication, hash operation, encryption operation and decryption operation based on ECC will be

Table 4: Comparison of security and function

| Scheme | Anonymity | Decentralization | Tamper-Resistant | System Scalability |
|---|---|---|---|---|
| *[13]* | √ | | | |
| *[22]* | √ | | | |
| *[6]* | √ | | | |
| *[15]* | √ | √ | √ | |
| *Our Scheme* | √ | √ | √ | √ |

involved, the computation overhead can be expressed as: $1T_H + 1T_{enc} + 1T_{dec}$. In authenticating, vehicles provide $H(Cert_{PID_i})$ to the RSU, and the RSU can authenticate legality of the vehicle by comparing with $H(Cert_{PID_i})_{block}$. Determining whether the message has been tampered with, we need to search its PID information and perform a hash operation. As shown in Figure 8, The time taken for 20 vehicles to complete the authentication is 5.245ms, The number of vehicles increased from 20 to 100, and the total time taken is 36.79ms.

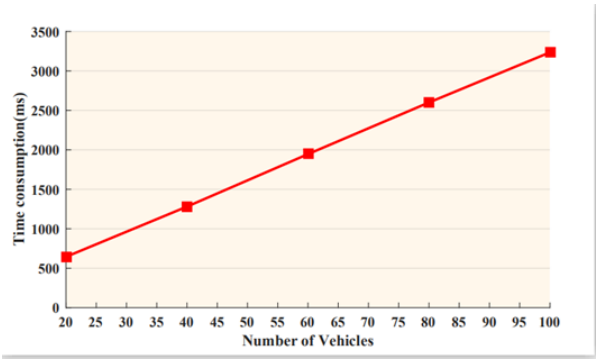


Figure 7: Registration of vehicle

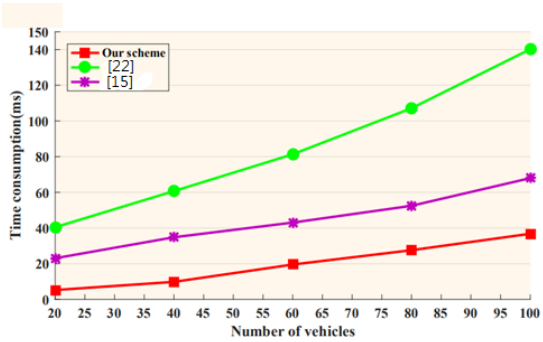


Figure 8: Authentication of vehicle

Figure 8 compares the time consumption of our scheme with [15, 22] under different values of n. Yao *et al.* [22] proposed an anonymous authentication scheme, seven encryption operations, six hash operations are required in their scheme. The scheme of [15] requires three encryption operations, two decryption operations, one hash operation. Compared with our scheme, their scheme authenticating 20 vehicles takes 40.454ms and 23.052ms respectively. In addition, the maximum time spent on authentication is 140.216ms in [22]. The results of simulation demonstrate that our proposal can meet the real-time performance of the VANETs.

For revocation, different from searching the complete certificate revocation list (CRL) bringing huge computational overhead, we introduce a revocation tab. Once the system considers that the vehicle is a malicious node, the PIDs stored on the trusted server will be marked with a tab. According to the blockchain, the RSU can determine whether the vehicle has been revoked by obtaining a $PID_i$ instead of $PID_i^{TAB}$.

In VANETs, many authentication schemes are based on the Bitcoin system. For example, in [15], they only store a certain number of bytes using the OP_RETURN instruction in bitcoin. In the Bitcoin system, Bitcoin developers believe that OP_RETURN will cause users to store too much non-transaction information in the Bitcoin network affecting the system performance of Bitcoin, therefore, the storage space is strictly restricted. However, with the number of vehicles increasing, the number of information stored in the blockchain will be enormous, which will directly affect the scalability of the system. In our scheme, only the pointer to $PID_i$ are stored in the blockchain, and the PID is stored in the trusted cloud server. The storage capacity of the trusted server is undoubtedly huge. Therefore, we do not worry about the storage problems caused by the explosion of vehicles.

In addition, as shown in Table 4, we compare it with schemes [6, 13, 15, 22] in terms of anonymity, tamper-resistant and decentralization. Our scheme has more advantages in security and function.

## 6 Conclusions

Aiming at providing a distributed security, in this paper, we propose an authentication scheme based on consortium blockchain with anonymous identity in VANETs. The anonymity of vehicles can be guaranteed by using PIDs to conceal the real identity of users. In order to improve the scalability of the system, we introduce a trusted cloud server to store the PIDs, and location pointers are uploaded to the blockchain. In addition, a vehicle can be considered an illegal node by judging whether the PID has a revocation tab instead of searching the entire certificate

revocation list (CRL). Finally, we analyze the security of our scheme and evaluate the performance of the anonymous authentication scheme.

## Acknowledgments

This work was supported by the Natural Science Foundation of China under Grants 61802303 and 61772418, the Innovation Ability Support Program in Shaanxi Province of China under Grant 2017KJXX-47, the Natural Science Basic Research Plan in Shaanxi Province of China under Grant 2016JM6033 and 2018JZ6001.

## References

[1] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017.

[2] F. Dötzer, "Privacy issues in vehicular ad hoc networks," in *International Workshop on Privacy Enhancing Technologies*, pp. 197–209, May 2005.

[3] K. K. Gai, M. K. Qiu, Z. G. Xiong, and M. Q. Liu, "Privacy-preserving multi-channel communication in edge-of-things," *Future Generation Computer Systems*, vol. 85, pp. 190–200, 2018.

[4] D. Y. Jia, K. J. Lu, J. P. Wang, X. Zhang, and X. M. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 263–284, 2016.

[5] D. Y. Jia and D. Ngoduy, "Enhanced cooperative car-following traffic model with the combination of V2V and V2I communication," *Transportation Research Part B: Methodological*, vol. 90, pp. 172–191, 2016.

[6] S. R. Jiang, X. Y. Zhu, and L. M. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 8, pp. 2193–2204, 2016.

[7] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.

[8] H. H. Kilinc and T. Yanik, "A survey of sip authentication and key agreement schemes," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 1005–1023, 2014.

[9] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. Ogah, and Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, 2017.

[10] Y. J. Li, "An overview of the DSRC/WAVE technology," in *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, pp. 544–558, Nov. 2010.

[11] C. L. Li, Y. Zhang, T. H. Luan, and Y. C. Fu, "Building transmission backbone for highway vehicular networks: Framework and analysis," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8709–8722, 2018.

[12] K. Lim and D. Manivannan, "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks," *Vehicular Communications*, vol. 4, pp. 30–37, 2016.

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

[14] Z. J. Lu, W. C. Liu, Q. Wang, G. Qu, and Z. L. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.

[15] N. Malik, P. Nanda, A. Arora, X. J. He, and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in *The 17th IEEE International Conference on Trust, Security And Privacy in Computing And Communications/12th IEEE International Conference on Big Data Science And Engineering (TrustCom/BigDataSE)*, pp. 674–679, 2018.

[16] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. (`https://bitcoin.org/bitcoin.pdf`)

[17] A. Nash, W. Duane, C. Joseph, D. Brink, *PKI: Implementing and Managing E-security*, 2001. ISBN 13: 978-0072131239.

[18] S. Rowan, M. Clear, M. Gerla, M. Huggard, C. M. Goldrick, "Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels," *arXiv Preprint arXiv:1704.02553*, 2017. (`https://arxiv.org/pdf/1704.02553.pdf`)

[19] H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, "Secure certificateless authentication and road message dissemination protocol in VANETs," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 13, 2018.

[20] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015–1028, 2015.

[21] Z. Yang, K. Yang, L. Lei, K. Zheng, and Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2018.

[22] L. Yao, C. Lin, G. W. Wu, T. Y. Jung, and K. B. Yim, "An anonymous authentication scheme in data-link layer for VANETs," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 22, no. 1, pp. 1–13, 2016.

[23] M. B. Younes, "Secure traffic efficiency control protocol for downtown vehicular networks," *International Journal Network Security*, vol. 21, no. 3, pp. 511–521, 2019.

[24] Y. Yuan and F. Y. Wang, "Towards blockchain-based intelligent transportation systems," in *IEEE 19th International Conference on Intelligent Transportation Systems (ITSC'16)*, pp. 2663–2668, Nov. 2016.

[25] T. Zhang and Q. Y. Zhu, "Distributed privacy-preserving collaborative intrusion detection systems for VANETs," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 148–161, 2018.

[26] D. Zheng, C. M. Jing, R. Guo, S. Y. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019.

[27] L. Y. Zhu, C. Chen, X. Wang, and A. O. Lim, "Smss: Symmetric-masquerade security scheme for VANETs," in *Tenth International Symposium on Autonomous Decentralized Systems*, pp. 617–622, Mar. 2011.

## Biography

**Liang Wang** received the B.S. degree from the Institute of Information Technology, GUET, in 2016. He is currently pursuing the M.S. degree with the National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, China. His research interests include anonymous authentication, vehicular ad hoc networks, and blockchain technology.

**Dong Zheng** received the Ph.D. degree from Xidian University, in 1999. He joined the School of Information Security Engineering, Shanghai Jiao Tong University. He is currently a Professor with the Xi'an University of Posts and Telecommunications, China. His research interests include information theory, cryptography, and information security. He is also a Senior Member of the Chinese Association for Cryptologic Research and a member of the Chinese Communication Society.

**Rui Guo** received the Ph.D. degree from the State Key Laboratory of Networking and Switch Technology, Beijing University of Posts and Telecommunications, China, in 2014. He is currently a Lecturer with the National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications. His current research interests include attribute-based cryptograph, cloud computing, and blockchain technology.

**ChenCheng Hu** received the B.Eng. degree from the Xi'an University of Posts and Telecommunications, in 2016, where he is currently pursuing the M.S. degree. He is doing research at the National Engineering Laboratory for Wireless Security. His current research interests include blockchain technology, user authentication, and information security.

**ChunMing Jing** received the bachelor's degree from the Xi'an University of Posts and Telecommunications, in 2017. He is currently pursuing the master's degree with the National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications. His research interests include blockchain technology, vehicular ad hoc networks, and security and privacy in the Internet of Things.