An Extensible and Effective Anonymous Batch Authentication Scheme for Smart Vehicular Networks

Jing Zhang, Hong Zhong, Jie Cui, Yan Xu, Lu Liu

***Abstract*—In recent years, research on the security of Industry 4.0 and the Internet of Things (IoT) has attracted close attention from industry, government and the scientific community. Smart vehicular networks, as a type of industrial IoT, inevitably exchange large amounts of security and privacy-sensitive data, which make them attractive targets for attackers. For protecting network security and privacy, we have proposed an extensible and effective anonymous batch authentication scheme. In contrast to traditional pseudonym authentication schemes, the same system private key need not to be preloaded in our scheme, effectively avoiding a system failure when destroying a vehicle. Besides, the certificate revocation list (CRL) size is merely related to the number of vehicles that have been revoked, regardless of the number of pseudonym certificates for revoked vehicles. Moreover, this scheme maintains the effectiveness of the traditional scheme, effectively reduces the scale of the CRL, and employs an identity revocation scheme that supports rapid distribution. The scheme supports conditional privacy protection, namely, only the trusted authority (TA) can uniquely trace and revoke vehicles. For illegal vehicles, the TA releases the two hashed seeds to facilitate traceability by all entities in its domain. Furthermore, security analysis indicates that our solution is secure under the random oracle model and fulfills a series of security requirements of vehicular networks. Compared to existing authentication schemes, performance evaluations show that the scheme offers relatively good performance in terms of time consumption.**

***Index Terms*—Industrial Internet of Things (IIoT), Pseudonym Authentication, Certificate Revocation List (CRL), Conditional Privacy Protection, Smart Vehicular Networks.**

I. Introduction

With the development of society and the progress and popularization of vehicle technology, the use of vehicles is continuously increasing [1], [2]. In 2018, the World Health Organization's "Global Status Report on Road Safety" pointed out that about 1.35 million people die from traffic accidents every year. Therefore, it is necessary to improve the driving experience and enhance driver safety, which leads to the research of vehicular networks [3], [4]. The typical structure of vehicular networks comprises three parts: a trusted authority (TA), a roadside unit (RSU) installed alongside the roads, and an on-board unit (OBU) equipped in vehicles. Communications in vehicular networks can be divided into two types: Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Infrastructure (V2I) communication. Both types of communications are carried out using the Dedicated Short Range Communications (DSRC) standard [5]. According to the DSRC protocol, each vehicle broadcasts a traffic message every $100-300$ ms in the communication range within 300 m. DSRC works in 5.9GHz band with bandwidth of 75MHz and approximate range of 1000 m [6]. Traffic messages generally include two types: road condition information and vehicle travel information. Road condition information contains road defects, traffic light interruptions, congestion conditions, etc., whereas vehicle travel information includes location, speed, waiting time, etc. [7], [8]. The receiver can make travel route adjustments based on the information received.

In addition to the above characteristics, the main difference of vehicular networks with traditional cellular network which use DSRC standard is the fact that the connection between vehicles (nodes) in the vehicular network is established in a short time, without any central infrastructure or base station [9], [10]. The network consists of some moving vehicles (nodes), which have no fixed location. In addition, vehicular network is a special mobile ad hoc network with vehicle as its node [11]. Vehicles can identify other vehicles around them to form a network by connecting to them and do necessary communications. Moreover, the high mobility of nodes is the main feature of this kind of network, which enables nodes to change their mode immediately [12]. The above characteristics make vehicular network become a promising technology of the modern intelligent transportation system.

Because of the wireless communication between entities, an attacker can control the communication channel fairly easily [13]. For example, an attacker can easily modify, replay, intercept and delete traffic-related messages transmitted in vehicular networks. These invalid messages can lead traffic control centers and receivers into making incorrect judgments and cause confusion and even traffic accidents and passenger casualties. Consequently, the security and integrity of traffic-related messages transmitted in vehicular networks are very important for many practical applications [14], [15]. For those vehicles that transmit their identity information to other entities in clear text, the travel route will be tracked by attackers by capturing traffic messages broadcast by these vehicles. The leakage of the travel route not only violates the driver's privacy, but may also endanger the safety of the driver and the passenger's life and property. However, when an illegal

J. Zhang, H. Zhong, J. Cui and Y. Xu are with the Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education, School of Computer Science and Technology, Anhui University, Hefei 230039, China, the Anhui Engineering Laboratory of IoT Security Technologies, Anhui University, Hefei 230039, China, and the Institute of Physical Science and Information Technology, Anhui University, Hefei 230039, China (e-mail: zhongh@ahu.edu.cn).

L. Liu is with the School of Informatics, University of Leicester, LE1 7RH, UK (email: l.liu@leicester.ac.uk).

vehicle sends misleading information, its real identity should be traced and revoked [16], [17]. Thus, conditional privacy-preserving schemes are urgently expected to solve the above problems.

In the past few years, researchers have put forward numerous conditional privacy-preserving authentication schemes [4], [18]–[24]. Among these, group signature based [19]–[21] and pseudonym-based authentication schemes [4], [22]–[24] can solve most security and privacy issues in vehicular networks. Nevertheless, as the network bandwidth and computing power of the vehicle are limited, the applicability of the above schemes is unacceptable [16], [18]. The revocation mechanism has two important performance metrics in vehicular networks [16]: verifying cost and size of the certificate revocation list (CRL). Unfortunately, high verifying overhead in the group signature based scheme is difficult to achieve for vehicles with limited computing power [25], whereas the huge CRL is easy to generate in the pseudonym-based authentication scheme [18]. While the CRL is broadcast to the vehicle, the CRL in the pseudonym-based authentication scheme results in high communication cost and occupies considerable storage space [26]. Therefore, it is vital to design a more efficient scheme that can not only meet the conditional privacy-preserving authentication, but also settle the shortcomings of CRLs in vehicular networks.

A. Research Background and Motivation

To address the above problem in vehicular networks, Raya et al. [27] designed a protocol for compressing the CRL using a Bloom filter. This compressed CRL is significantly shorter than the traditional CRL, with consequent reduction in storage and verifying cost. However, the false positives of the Bloom filter may cause legitimate vehicles to be erroneously revoked. In this scheme, the roadside unit (RSU) needs to broadcast the latest parameters that have been revoked to all legitimate vehicles in time to facilitate the update of the Bloom filter. In recent years, some work has emerged [16], [28], [29], involving the use of short-term certificates and regional management to reduce the number of entries in the CRL. Unfortunately, these studies ignore the fact that inspections in open networks can lead to loss of privacy. In addition, the full network broadcast of the CRL cannot satisfy the rapid demand of the surrounding vehicles of the cancelled vehicle.

To address the disclosure of privacy information and message integrity issues, digital signature public key infrastructure [30]–[32] is a good choice. Unfortunately, because of the vehicle's lack of computing power, it is difficult to process all authentications in a short period of time, particularly in places with high traffic density. Besides, verifying messages from unidentified vehicles involves transmitting public key certificates, which results in a large amount of computational cost. Consequently, nearby RSUs are assigned to verify the messages. Because the number of signatures that need to be verified can be very large, an efficient way to conduct batch verification is urgently needed.

Although numerous authentication schemes [13], [33], [34] using batch signatures have been proposed, they all rely on a tamper-proof device to store the system private key. Once a vehicle's device is attacked by a side channel attack, the entire system is undermined [19], [35]. At the same time, if the system private key in a device is obtained, then anyone can trace the true identity of any vehicle. In addition, in terms of efficiency, if one of the signatures is wrong during the batch verification process, the entire batch will be discarded. Although valid signatures constitute a large proportion in a batch, discarding batches is inefficient and may mean an unsatisfactory success rate.

Another challenge in vehicular networks is that vehicle speeds are high whereas their communication range is short, which results in limited communication time between the RSU and the vehicles [36]. Although existing solutions can achieve satisfactory performance in a batch authentication way, with the exponential growth of messages and CRLs, these schemes cannot achieve timely fast authentication. Mainly because of the complex operation of bilinear pairing and MapToPoint, these schemes are inefficient at handling batch message authentication [26]. Therefore, to reduce computational cost, conditional privacy-preserving authentication schemes based on elliptic-curve cryptosystems are generally accepted [13], [34], [37].

The motivation for our research is mainly expressed in the following aspects: 1) References [35] and [19] make us realize that the research on resistance of side channel attack is important and of great practical significance. For example, References [13] and [33] store the system key s into the tamper-proof device. Once a vehicle is attacked by the adversary to obtain s, the whole system will disorder. Therefore, it is necessary to design a good scheme to hide the private key (see Section III.C). 2) According to the DSRC standard [5], we know that the communication range of the vehicle is 300m, and that of the base station is 1000m. For example, when a malicious vehicle or RSU is suddenly revoked, the malicious message broadcast by it may still be forwarded. Therefore, it is necessary to design a certificate revocation mechanism to meet the requirements of rapid distribution in order to reduce the harm of revoked vehicles or RSUs (see Section III.F).

B. Our Contributions

To deal with the above-mentioned problems, we design an extensible and effective anonymous batch authentication scheme for vehicular networks. We use elliptic-curve cryptography to reduce the computational overhead of batch authentication. The main contributions of this work are as follows:

1) First, we propose an extensible and effective anonymous batch authentication scheme to generate the pseudoidentities pertaining to the same vehicle based on a one-way hash-chain for vehicular networks. In contrast to traditional pseudonym authentication schemes, the proposed scheme does not rely on hardware devices, effectively avoiding side channel attacks.
2) Second, we provide an identity revocation scheme that supports rapid distribution. The CRL size in the proposed scheme is related only to the number of vehicles that are revoked, regardless of the number of pseudonym certificates for vehicles that have been revoked.

3) Third, we design a conditional privacy protection authentication scheme. Only the TA can uniquely trace anonymous vehicles. For illegal vehicles, the TA releases two hashed seeds to facilitate traceability by all entities in its domain.
4) Finally, through security proof and performance evaluation, we analyze the security strength and time consumption indicators of the proposed authentication scheme.

C. Organization of the Rest Paper

Section II shows the preliminaries, network structure and some security requirements. Section III expresses the detailed scheme. Section IV provides security proof and security analysis. Then the performance evaluation is shown in Section V. Finally, some concluding remarks are provided in Section VI.

II. System Models and Objectives

In this section, we will focus on some preliminaries, the network architecture, and some security and privacy requirements that will be used in next section.

A. Preliminaries

In this subsection, we introduce some preliminaries, including secure hash chains [38] and elliptic curve cryptosystem [39], which are the bases of our proposed scheme.

1) Hash Chains: A one-way hash function $h(\cdot)$ is said to be secure if the following properties are satisfied:

- $h(\cdot)$ can input any length of message to produce a fixed length output.
- Given x, it is easy to calculate $h(x) = y$. Conversely, given y, it is hard to calculate $h^{-1}(y) = x$.
- Given x, it is computationally infeasible to find $x \neq x^{'}$ such that $h(x) \neq h(x^{'})$.

Assume that $h^i(x) = h(h^{i-1}(x))$, a hash chain of length L is defined in Fig. 1, where SD is an initial seed value and $S_i = h^i(SD)$, $i \in [1, L]$. Obviously, given S_{i-1}, it is easy to calculate $S_i = h(S_{i-1})$, but infeasible to gain S_{i-2}.

Fig. 1. Hash chain.

2) Elliptic Curve Cryptosystem: Let $q > 3$ be a large prime which is used to determine a finite F_q. Let $E_{a,b}$ denotes the group of points of the elliptic curve $E_{a,b}$: $y^2 = x^3 + ax + b(\mathrm{mod}q)$ over the finite field F_q , where $a, b \in F_q$ and $4a^3 + 27b^2(\mathrm{mod}q) \neq 0$. Let $G_p = \langle P \rangle$ be a cyclic group of prime order p, where P is a generator point of the group and $P \in E_{a,b}(F_q)$.

The security of the proposed scheme relies on solving the elliptic curve discrete logarithm (ECDL) mathematical problem. The ECDL is a "hard" problem, given $Q = sP$, where P ,Q belong to a curve $E_{a,b}$. It is "easy" to compute Q given s and P, but "hard" to find s given P and Q.

B. Network structure and components

In this part, we introduce our vehicular network structure model, which is consists of three network components: vehicle, roadside units (RSUs) and system trusted authority (TA). The wireless communication in this network structure can be mainly classified into the following three types, RSU-to-vehicle communication, vehicle-to-RSU communication, and vehicle-to-vehicle communication. Other communications are via secure wired channels such as RSU-to-TA communications and TA-to-RSU communications. In the following, we discuss the network components in Fig. 2.

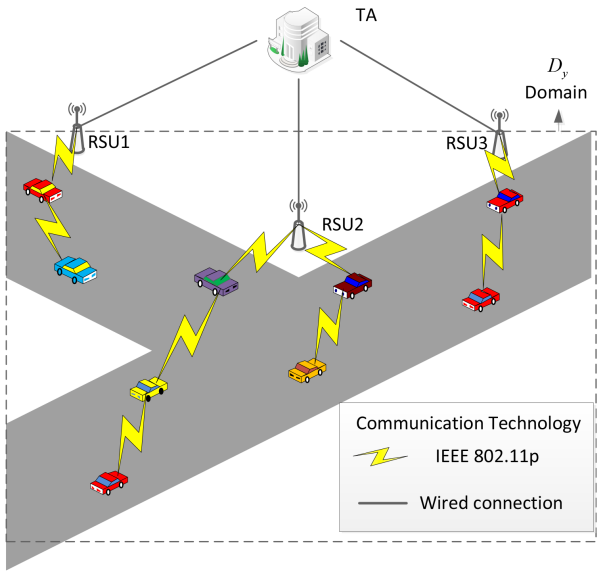


Fig. 2. The system model for smart vehicular networks.

- TA: Assume that TA has high credibility and sufficient storage and computation capacity. The TA divides the scope it governs into several domains and generates the system's master private key, the system public key as well as public parameters for each domain. It also generates a series of pseudonyms and its corresponding private keys for each vehicle. TA generates a unique certificate for the RSU in its domain, and delivers its sensitive information to them via secure channels. Moreover, TA has two certificate revocation lists $CRL_{D_y,R}$ and $CRL_{D_y,V}$ for managing the compromised RSUs and the illegal vehicles in the D_y, respectively.
- RSU: It acts as an intermediary between the vehicle and the TA. It is connected to the TA via a secure wired link. The RSU communicates with the vehicle over a wireless link. And it in charge of verifying vehicles' identity.
- Vehicles: Each vehicle is equipped with an onboard unit (OBU), which is primarily responsible for communicating with each other to share traffic information. It is considered that the energy of the vehicle is sufficient. Each vehicle has a tamper-proof module (TPM) for storing sensitive information received from TA.

C. Security and Privacy Requirements

Based on the system models and components shown in Fig. 2, we describe the security and privacy requirements, as follows.

1) ***Authentication and message integrity:*** Authentication ensures that the receiver can verify the authenticity of the sender. In addition, message integrity further ensures that the content of the message has not been altered during transmission.
2) ***Identity revocation:*** To exclude unexpired illegal vehicles or compromise RSU from vehicular networks.
3) ***Un-linkability:*** No adversary can link two messages generated by the same vehicle.
4) ***Backward privacy:*** A revoked member cannot be tracked by other members during the time period before the revocation takes effect.
5) ***Replay attack:*** Even if a malicious attacker gets a legal message, it can not add the timeslot of the message and forward it at the later time to threaten the traffic safety.

III. The Proposed Scheme

In this section, we will introduce the proposed scheme from six phases: system initialization, RSU's certificate issuing, vehicle's certificate issuing, vehicle message signing, message verification, and identity revocation and rapid distribution. Table I shows the notations of the proposed scheme.

TABLE I
Notations and Definitions Used

Notations	Definitions
TA	The trusted authority
R_x	The x-th roadside unit
V_i	The i-th vehicle
s	The master secret key
P_{pub}	The system public key
ΔT	The validity period of pseudonym certificate
D_y	The y-th domain
$Cert_{A,B}$	The certificate of B issued by A
γ, k, μ	Random numbers
sk_{R_x}	The private key of R_x
PK_{R_x}	The public key of R_x
$\sigma_{A,B}$	The signature of B issued by A
$Sign(A,B)$	Signing B by Schnorr signature algorithm with A
TS_j	The j-th time slot that ends at $j * \Delta T$
VP_A	The certificate validity period of A
$PID_{i,j}$	The pseudoidentity of V_i in j-th time slot
$sk_{i,j}$	The private key corresponding to $PID_{i,j}$
T_i	The current imestamp
M_i	The message sent by V_i
$CRL_{A,B}$	The certificate revocation list of B in domain A
h	The secure hash function
$\oplus$	The exclusive-OR operation
$\|\|$	The concatenation operation

A. System Initialization Phase

Given the parameters of elliptic curve (G, q, P), TA runs the following steps to initialize system parameters.

1) TA picks a random number $s \in Z_q^*$ as the master private key, and then computes the corresponding system public key $P_{pub} = s \cdot P$.
2) TA selects two one-way hash function $h_i : \{0,1\}^* \rightarrow Z_q^*$, $i = 1, 2, 3$.
3) TA selects ΔT and sets it as the validity period of the pseudonym certificate. According to the density of the R_x, the TA estimates the number of certificates updated in the domain D_y, which is expressed as L_w.
4) Then, TA publishes system parameters $params = \{G, q, Z_q^*, P_{pub}, h_i, \Delta T, L_w\}$.

B. RSU's Certificate Issuing Phase

TA is divided into several domains, each of which contains multiple RSUs. The following steps describe the process by which the TA issues a certificate $Cert_{TA,R_x}$ for R_x in domain D_y.

1) TA generates a random number sk_{R_x} as the private key of R_x, and sets the corresponding public key $PK_{R_x} = sk_{R_x} P$.
2) TA sets the signature $\sigma_{TA,R_x} = Sign(PK_{R_x} || D_y)$ which is used for verification of the R_x by passing vehicles.
3) TA stores and forwards sk_{R_x} and certificate $Cert_{TA,R_x}$ to R_x via a secure channel, where $Cert_{TA,R_x} = (D_y, PK_{R_x}, \sigma_{TA,R_x})$.

C. Vehicle's Pseudonyms and Private Keys Generation Phase

It is assumed that vehicles can obtain a series of pseudonyms from the TA during the vehicle inspection, and pre-store in the vehicle registers [16]. Denote TS_j as j-th time slot that ends at $j * \Delta T$, which can be divided into C time slots for one year. Suppose the TA issues $L_w * C$ pseudonymous certificates $Cert_{TA,V_{i,j}}$ for the vehicle V_i at the time slot TS_j ($j \in [1, L_w * C]$), where its validity period $VP_{V_{i,j}} = j$.

1) From formula (1) we can see that the pseudoidentity $PID_{i,j}$ of $Cert_{TA,V_{i,j}}$ is generated by two hash chains.

$$\begin{cases} S_{1,j} = h_1^j(SD_{i,1}) \\ S_{2,C*L_w-j+1} = h_1^j(SD_{i,2}) \\ PID_{i,j} = h_1^j(S_{1,j} \oplus S_{2,C*L_w-j+1}) \end{cases} \quad (1)$$

2) For generating a private key $sk_{i,j}$, TA randomly selects $k_i \in Z_q^*$, and computes $K_{i,j} = k_i P$, $h_{i,j} = h_1(PID_{i,j}, K_{i,j}, TS_j)$ and $S_{i,j} = k_i + h_1(PID_{i,j}, K_{i,j}, TS_j) \cdot s \ mod \ q$. Then, TA sets private key $sk_{i,j} = (K_{i,j}, S_{i,j})$.
3) The TA delivers pseudoidentity $PID_{i,j}$ and its corresponding private keys $sk_{i,j}$ to the vehicle V_i via a secure channel.

Remark: In order to avoid the side channel attack, one can use the random secret k_i for a vehicle V_i as $S_{i,j} = k_i + h_1(PID_{i,j}, K_{i,j}, TS_j) \cdot s \ mod \ q$. Even if the attacker obtains the private key $S_{i,j}$ through a series of physical attacks, without knowing the secret k_i, he/she cannot get the master private key s.

D. Vehicle Message Signing Phase

R_x broadcasts its certificate $Cert_{TA,R_x}$ every 5 seconds in domain D_y. If the vehicle V_i enters a new domain D_y and receives a message $Cert_{TA,R_x}$ from the RSU, it will verify $Cert_{TA,R_x}$ by formula (2).

$$Verify(P_{pub}, D_y, PK_{R_x}, \sigma_{TA,R_x}) \tag{2}$$

If $Cert_{TA,R_x}$ is valid, the vehicle V_i generates a signature σ_i for the traffic-related message M_i by the following steps.

1) V_i selects a number $\mu \in Z_q^*$ randomly, and calculates $U_{i,j} = \mu_{i,j}P$.
2) V_i randomly choose a pseudoidentity $PID_{i,j}$ and its corresponding private keys $sk_{i,j}$, and computes $h_{i,j}^* = h_2(PID_{i,j}, K_{i,j}, U_{i,j}, M_i, T_i)$, $\delta_{i,j} = S_{i,j} + h_2(PID_{i,j}, K_{i,j}, U_{i,j}, M_i, T_i) \cdot \mu \ mod \ q$, where $T_i \in [TS_{j-1} \cdot \Delta T, TS_j \cdot \Delta T]$ is a current timestamp.
3) The vehicle V_i sets the signature $\sigma_i = (K_{i,j}, U_{i,j}, \delta_{i,j})$ on the M_i and the T_i for $PID_{i,j}$, and sends $\{\sigma_i, M_i, T_i, PID_{i,j}\}$ to R_x.

E. Message Verification Phase

The RSU can verify a batch of signatures σ_i on the M_i and the T_i for $PID_{i,j}$, where $i = 1, 2, ..., n$. Upon receiving n distinct message-signature tuples $PID_{i,j}, \sigma_i, M_i, T_i$, the R_x needs to do the following steps to verify the validity of this batch of signatures.

1) R_x first checks whether $PID_{i,j}$ is in the CRLs. If $PID_{i,j}$ is not in CRLs, R_x continues the following steps.
2) R_x requires to get the time slot TS_j from T_i, and computes $h_{i,j} = h_1(PID_{i,j}, K_{i,j}, TS_j)$, $h_{i,j}^* = h_2(PID_{i,j}, K_{i,j}, U_{i,j}, M_i, T_i)$.
3) To overcome the non-repudiation attack, R_x uses the small exponent test technology [40] to verify whether this batch of signatures is holds by equation (3), where $x_i \in [1, 2^l]$, and l is a small integer.

$$\begin{aligned}(\sum_{i=1}^{n} x_i\delta_{i,j})P = (\sum_{i=1}^{n} x_i h_{i,j}^* U_{i,j}) + \sum_{i=1}^{n} x_i K_{i,j} \\ +(\sum_{i=1}^{n} x_i h_{i,j})P_{pub}\end{aligned} \tag{3}$$

If the equation is true, it indicates that these distinct n signatures are legal. Next, we analyse the correctness of the batch messages verification using equation (4). Due to $\mathrm{P}_{pub} = s \cdot \mathrm{P}$, $K_{i,j} = k_i P$, $U_{i,j} = \mu_{i,j}P$, $h_{i,j} = h_1(PID_{i,j}, K_{i,j}, TS_j)$, $h_{i,j}^* = h_2(PID_{i,j}, K_{i,j}, U_{i,j}, M_i, T_i)$, $S_{i,j} = k_i + h_1(PID_{i,j}, K_{i,j}, TS_j) \cdot s \ mod \ q$, $\delta_{i,j} = S_{i,j} + h_2(PID_{i,j}, K_{i,j}, U_{i,j}, M_i, T_i) \cdot \mu \ mod \ q$ and $\sigma_i = (K_{i,j}, U_{i,j}, \delta_{i,j})$, we obtain

$$\begin{aligned}&\left(\sum_{i=1}^{n} x_i\delta_{i,j}\right) \cdot P = \left(\sum_{i=1}^{n} x_i \cdot \left(S_{i,j} + h_{i,j}^* \cdot \mu\right)\right) \cdot P \\ &= \left(\sum_{i=1}^{n} x_i \cdot \left(k_i + h_{i,j} \cdot s + h_{i,j}^* \cdot \mu\right)\right) \cdot P \\ &= \left(\sum_{i=1}^{n} x_i \cdot \left(k_i \cdot P + h_{i,j} \cdot s \cdot P + h_{i,j}^* \cdot \mu \cdot P\right)\right) \\ &= (\sum_{i=1}^{n} x_i h_{i,j}^* U_{i,j}) + \sum_{i=1}^{n} x_i K_{i,j} + (\sum_{i=1}^{n} x_i h_{i,j})P_{pub}\end{aligned} \tag{4}$$

F. Identity Revocation and Rapid Distribution Phase

In the proposed scheme, the TA releases the CRLs to the revoke the illegal vehicles and RSUs in every domain. We denote the compromised RSUs and the illegal vehicles in the D_y by $CRL_{D_y,R}$ and $CRL_{D_y,V}$, respectively. Based on the DSRC standard [5], each vehicle broadcasts a traffic-related information every 100-300 ms, which includes location, speed and other information. In addition, the range of communication between nodes in vehicular networks is limited. Therefore, the location of the reporter or the monitoring equipment can be directly used to represent the location X of the illegal vehicle. For the certificates that have been stored in the CRLs, we adopt the following methods for rapid distribution.

[Revoke Illegal Vehicles]

To revoke a illegal vehicle V_i in D_y, the TA adds its pseudonymous certificate to $CRL_{D_y,V}$, and informs to all RSUs and all vehicles in V_i's communication range by the following steps.

1) From the 5-tuple $\langle V_i, 0, C, SD_{i,1}, SD_{i,2}\rangle$, TA finds out the maximum time period of $\{m\}$, where $m \in (n, C]$, and the current time denotes $\{n * L_w\}$. If $n \neq m$, TA computes the formula (5). Then, it adds the 4-tuple $\langle (n-1) * L_w, m * L_w, S_{1,(n-1)*L_w+1}, S_{2,(C-m)*L_w+1}\rangle$ into the $CRL_{D_y,V}$.

$$\begin{cases} S_{1,(n-1)*L_w+1} = h_1^{(n-1)*L_w+1}(SD_{i,1}) \\ S_{2,(C-m)*L_w+1} = h_1^{(C-m)*L_w+1}(SD_{i,2}) \end{cases} \tag{5}$$

2) TA calculates the influence time period Δt of the illegal vehicle based on the time t_1 contained in the report information and the time t_2 at which the information is received, where

$$\Delta t = t_2 - t_1 \tag{6}$$

Assuming long-term monitoring in an domain shows that 90% of the vehicle's speed does not exceed V_{max}, then V_{max} can be selected as the maximum speed at which the vehicle moves. Note that if a violating vehicle attempts to travel beyond the set maximum speed to send false messages to attack the network, it will be subject to restrictions such as traffic regulations.

3) TA calculates the distance L that the violating vehicle V_i can travel in the influence period Δt, where

$$L = \Delta t \cdot V_{max} \tag{7}$$

Let's estimate influence distance in the worst case. As shown in Fig. 3, V_i driving in a certain direction Δt, a vehicle V_x driving in the opposite direction Δt, the V_i and V_x meet. V_x is exactly the farthest vehicle that V_i can affect. Therefore, the farthest influence distance is:

$$D = 2L \tag{8}$$

Therefore, the maximum influence of illegal vehicle is:

$$S = \pi D^2 = 4\pi(\Delta t \cdot V_{max})^2 \tag{9}$$

4) After estimating the maximum impact range of V_i, the TA first notifies all RSUs and vehicles covered by this

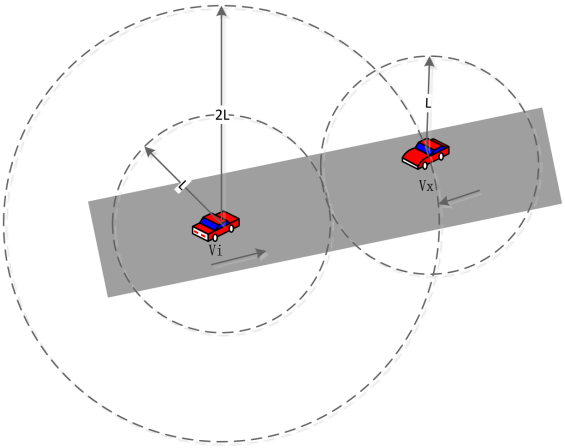


Fig. 3. The maximum impact range of illegal vehicles.

range. These RSUs add the certificate revocation 4-tuple of V_i to the CRL that needs to be broadcast, and release it when the CRL is released next time. Moreover, any vehicle can compute the pseudoidentities $PID_{i,j}$ of the revoked pseudonymous certificates:

$$\begin{cases} S_{1,j} = h_1^{j-(n-1)*L_w-1}(S_{1,(n-1)*L_w+1}) \\ S_{2,C*L_w-j+1} = h_1^{m*L_w-j}(S_{2,(C-m)*L_w+1}) \\ PID_{i,j} = h_1^{j}(S_{1,j} \oplus S_{2,C*L_w-j+1}) \end{cases} \quad (10)$$

Moreover, the pseudoidentities $PID_{i,j}$ used in the time slot TS_j will be added into its local CRL by vehicle.

[Revoke Compromised RSUs]

To revoke a compromised RSU R_x in D_y, the TA adds its certificate into $CRL_{D_y,R}$, and informs to all RSUs and all vehicles in R_x's communication range by the following steps.

1) TA calculates the influence time period $\Delta t = t_2 - t_1$ of the compromised RSU based on the time t_1 contained in the report information and the time t_2 at which the information is received.
2) TA computes the travel distance L_R of the affecting vehicle V_m by the compromised R_x in the influence period Δt, where

$$L = \Delta t \cdot V_{max} \quad (11)$$

Let's estimate influence distance in the worst case. As shown in Fig. 4, V_x is exactly the farthest vehicle that V_m can affect. Therefore, the farthest influence distance is:

$$D = 2L + r \quad (12)$$

Therefore, the maximum influence of compromised RSU R_x is:

$$S = \pi D^2 = \pi(2\Delta t \cdot V_{max} + r)^2 \quad (13)$$

3) After estimating the maximum impact range of R_x, the TA first notifies all RSUs and vehicles covered by this range. These RSUs add the certificate revocation of R_x to the CRL that needs to be broadcast, and release it when the CRL is released next time.

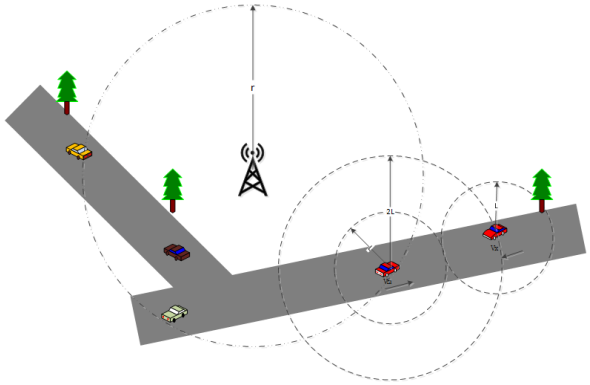


Fig. 4. The maximum impact range of compromised RSUs.

IV. Security Proof and Analysis

We show that our scheme is secure in this section. Moreover, detailed security analysis shows that our proposed solution can resist multiple ordinary attacks.

A. Security Proof

Here, we prove our scheme is secure with the random oracle model, and the security model is defined by a game played between a simulator B and an adversary A.

- Setup Oracle: B generates the system parameters and the system private key. Then, B sends the system parameters to A.
- h_1 Oracle: B randomly selects a number $\tau \in Z_q^*$, and inserts (m, τ) into the list L_{h_1}. Then, B sends τ to A.
- h_2 Oracle: B randomly selects a number $\tau \in Z_q^*$, and inserts (m, τ) into the list L_{h_2}. Then, B sends τ to A.
- Extract Oracle: Upon receiving the message $PID_{i,j}$, B generates a message $(PID_{i,j}, S_{i,j})$ and returns it to A.
- Sign Oracle: Once get the message M_i, B generates a message $(\sigma_i, M_i, T_i, PID_{i,j})$ and sends it to A.

The A could violate the proposed scheme Γ, if A generates a valid login request message. Let $Adv^{Auth}(A)$ denote the probability that A could violate the proposed scheme.

Theorem 1: Let Q denote the number of queries that A asks to the random oracle and R represents the number of queries that A asks to the sign oracle, respectively. If A can break the proposed scheme, the simulator B can break ECDL problem within a time period T, where $T < 120686QT/\varepsilon$ and $\varepsilon \geq 10(R+1)(R+Q)/q$.

Proof: Assumed that there exists an adversary A who has the capability to forge a message $(\sigma_i, M_i, T_i, PID_{i,j})$. And a simulator B which can solve the ECDL problem with a non-negligible probability by utilizing A as a subroutine, is constructed. Notice that B maintains hash lists L_{h_1} and L_{h_2}.

Setup: B selects a number s randomly as its private key and computes $P_{pub} = sP$. Next, it sends the parameters $params = \{G, q, Z_q^*, P_{pub}, h_1, h_2, \Delta T, L_w\}$ to A.

h_1 *Oracle:* Once get A's query with the message $(PID_{i,j}, K_{i,j}, TS_j)$, B checks whether parameter $(PID_{i,j}, K_{i,j}, TS_j, \tau)$ exists in the hash list L_{h_1}. If yes, B sends τ to A; otherwise, B randomly selects a number

$\tau \in Z_q^*$, and inserts the tuple $(PID_{i,j}, K_{i,j}, TS_j, \tau)$ into the list L_{h_1}. Then, B returns τ to A.

h_2 *Oracle:* Once get A's query with the message $(PID_{i,j}, K_{i,j}, U_{i,j}, M_i, T_i)$, B checks whether parameter $(PID_{i,j}, K_{i,j}, U_{i,j}, M_i, T_i, \tau)$ exists in the hash list L_{h_2}. If so, B sends τ to A; otherwise, B randomly selects a number $\tau \in Z_q^*$, and inserts the tuple $(PID_{i,j}, K_{i,j}, U_{i,j}, M_i, T_i, \tau)$ into the list L_{h_2}. Then, B returns τ to A.

Extract Oracle: If A conducts an extract query on a vehicle's identity $PID_{i,j}$, B computes $K_{i,j} = k_i P$ and checks if the tuple $(PID_{i,j}, K_{i,j}, TS_j)$ exists in the L_{h_1}. If yes, B computes $S_{i,j} = k_i + h_1(PID_{i,j}, K_{i,j}, TS_j) \cdot s \ mod \ q$ and the value $S_{i,j}$ is outputted to A. Otherwise, B sends a failure message to A and refuses this query. Note that A cannot get $S_{i,j}$ of the targeted victim (vehicle) with $PID_{i,j}$ through this extract query.

Sign Oracle: If A conducts a sign query on message M_i under a vehicle's identity $PID_{i,j}$, B checks if the tuple $(PID_{i,j}, K_{i,j}, TS_j)$ exists in the hash list L_{h_1}. B gets τ from L_{h_1} and chooses two random numbers μ_i and h_i. Then, B chooses α_i and β_i randomly and tries again. Otherwise, B generates $U_i = h_i^{-1}\alpha_i P - Q$ and $\delta_i = \alpha_i$. Next, B sends (M_i, U_i, δ_i) to A, where $h_i = h_2(PID_{i,j}, K_{i,j}, U_{i,j}, M_i, T_i)$.

Analysis: Through Forking Lemma [41], we can know that, If A construct two valid signatures $(U_i, \delta_i = h_i \cdot \mu_i + S_{i,j} \bmod q)$ and $(U_i, \delta_i^{'} = h_i^{'} \cdot \mu_i + S_{i,j} \bmod q)$ successfully, and $h_i \neq h_i^{'}$, B can get $S_{i,j}$ by computing

$$\begin{aligned} &\frac{h_i^{'}\delta_i - h_i\delta_i^{'}}{h_i^{'} - h_i} \bmod q \\ &= \frac{h_i^{'}h_i\mu_i + h_i^{'}S_{i,j} - h_i h_i^{'}\mu_i - h_i S_{i,j}}{h_i^{'} - h_i} \bmod q \\ &= S_{i,j} \end{aligned} \tag{14}$$

B can solve the ECDL problem within time T, where $T < 120686QT/\varepsilon$, if $\varepsilon \geq 10(R+1)(R+Q)/q$. Therefore, the proposed authentication scheme is secure in the random oracle model.

B. Security Analysis

We will show that the proposed scheme meet all security and privacy requirements described in Section 2, in this subsection.

1) ***Authentication and message integrity:*** Based on Theorem 1, we have known that Γ is secure against adaptive chosen $PID_{i,j}$ attack and adaptive chosen message attack under random oracle because the ECDL problem is hard. In addition, we uses the signature algorithms to sign messages in the communication process. Messages sent by vehicles contains the signatures σ_i which are signed using TA's private key and itself own private key. $Cert_{TA,R_x}$ which broadcasted by R_x contains σ_{TA,R_x} which is also signed using TA's private key. It is obvious that computing TA's private key is an example of the ECDL problem. Therefore, the communication process is authentication and message integrity.
2) ***Identity revocation:*** In our scheme, the TA can preclude a compromised RSU or an illegal vehicle from the vehicular networks through revoking its unexpired certificates with a CRL. For preventing an illegal vehicle from access the networks, TA needs to release two hash elements $S_{1,j}$, $S_{2,C*L_w-j+1}$ only, which correspond to the revocation time slot TS_j. Other participants can calculate the revoked vehicles' pseudoidentities and discard the messages which signed using those certificates.
3) ***Un-linkability:*** In the proposed authentication scheme, attackers cannot link two pseudonyms sent from the same vehicle. To extract the relationship of two pseudoidentities $PID_{i,j} = h_1^j(S_{1,j} \oplus S_{2,C*L_w-j+1})$ and $PID_{i',j+1} = h_1^{j+1}(S_{1,j+1} \oplus S_{2,C*L_w-j})$, the attack should firstly calculate $x = h_1^{-1}(S_{1,j} \oplus S_{2,C*L_w-j+1})$ and $y = h_1^{-1}(x \oplus S_{1,j})$ for each possible value of $S_{1,j}$ until the condition $h_1(h_1(S_{1,j} \oplus y)) = PID_{i',j+1}$ is establish. For a 224-bit one-way hash function, for instance, hash function $SHA-2$, the expected cost of solving h_1^{-1} is $O(2^{224-1})$. Suppose $PID_{i,j}$ and $PID_{i',j+1}$ belong to the same vehicle, the relationship of two pseudoidentities needs 2^{446} times of operations to validate, that is, it is a difficult computational problem to link the relationship between two pseudonyms.
4) ***Backward privacy:*** In the proposed authentication scheme, it is hard for any third party to get pseudoidentities used by the revoked vehicle. Suppose $S_{1,j}$ and $S_{2,C*L_w-j+1}$ are released to revoke a vehicle V_i at the time slot TS_j. In order to compute V_i's pseudoidentity $PID_{i,j-1} = h_1^{j-1}(S_{1,j-1} \oplus S_{2,C*L_w-j+2})$ in the time slot TS_{j-1}, the attacker has to know $S_{1,j-1} = h_1^{-1}(S_{1,j})$ at first. For a 224-bit one-way hash function, it is impossible to get $S_{1,j-1}$ from $S_{1,j}$.
5) ***Replay attack:*** Messages M are contain a timestamp TS, the participant can discover the replay attacks by verifying the validity of the timestamp TS. That is, our scheme can resist the replay attack.

V. Performance Evaluation

Here, we will show that the proposed scheme can meet the requirements of the vehicular network. All eight safety-related applications and their latency requirements [42], [43] are shown in Table II. First of all, we will introduce the contributions and shortcomings of the four state-of-art authentication schemes [4], [18], [22], [23]. Next, we will analyze the proposed authentication scheme with these four state-of-art authentication schemes in terms of computation cost and communication cost. Besides, we will carry out simulation experiments in the aspect of the average transmission delay to prove that our scheme achieves better performance.

In [18], Jiang et al. presented a new CRL-based scheme, called anonymous batch authentication (ABAH). When the vehicle received a message, the certificate revocation list (CRL) inspection process will run before the certificate and signature verification in the vehicle network. However, due to the complex operation of bilinear pairing and mapping points, the scheme is inefficient in processing batch message authentication. For example, when the number of messages reaches 100, the verification overhead of the verifier reaches 357.27ms.

TABLE II
EIGHT ACTIVE SAFETY LATENCY REQUIREMENTS

Safety Applications	Latency (milliseconds)
Traffic signal violation warning	100
Curve speed warning	1000
Emergency electronic brake lights	100
Precrash sensing	20
Cooperative forward collision warning	100
Left turn assistant	100
Lane change warning	100
Stop sign movement assistance	100

In [22], Azees et al. proposed an efficient message authentication scheme for VANETs. In their scheme, the malicious vehicle can be detected and avoided to enter into the VANETs, and an RSU can efficiently authenticate vehicles in the anonymous manner before sending location based service messages to nearby vehicles. And their proposed scheme can achieve low message authentication cost and support easy revocation. However, this scheme also has the disadvantage of large computation and communication overhead.

Li et al. [23], by using the pseudo-identity method [37], constructed an anonymous conditional privacy-preserving authentication scheme. In this scheme, each OBU should restore a large number of pseudo-identities to keep the privacy of its identity. However, under this scheme, both the TRA and PKG need to be added at the same time, and multiple TRAs can make the vehicle tracking and revocation process to be more complex and be detrimental for protocol extensions.

Chinese remainder theorem (CRT)-based conditional privacy-preserving authentication scheme [4], called PA-CRT, is our recently proposed scheme. This scheme can well protect the system's private key, and has very low computation overhead and communication overhead. However, we now notice that most vehicles are offline when they are not moving. If the domain key is updated, an offline vehicle cannot guarantee the timely update of the domain key. So now the proposed scheme is applicable to both online and offline states. In order to better protect the system private key, the vehicle needs to use the ciphertext of the system private key to participate in the computation and communication, so the cost of the proposed scheme is slightly lower than the scheme [4]. Specific details are compared below.

A. Computation Cost Analysis

To compare and analyze the schemes, we adopt the same execution time as in [4]. The execution time of cryptographic operations have been obtained using MIRACL library [44] on the hardware platform which contains 4 gigabytes memory, an Intel I7-4770 processor, and runs on Windows 7 operating system. Table III lists out the time of executing following cryptographic operations.

Table IV represents the computational cost required for each step of the vehicle authentication process for various schemes. To research the bilinear pairing characteristics [18], [22] and the ECC-based characteristic [4], [23] efficiency in vehicular networks, we focus on the analysis of the ABAH [18] and the proposed schemes.

TABLE III
EXECUTION TIME OF CRYPTOGRAPHIC OPERATIONS

Symbol	Description	Time (milliseconds)
T_{bp}	Bilinear pairing operation $e(\bar{P}, \bar{Q})$, where $\bar{P}, \bar{Q} \in G_1$. (G_1 is additive group)	4.2110
$T_{bp.m}$	Scale multiplication operation $a \cdot \bar{P}$ related to the bilinear pairing, where $a \in Z_q^*$.	1.7090
$T_{bp.sm}$	Small scale multiplication operation $x \cdot \bar{P}$ related to the bilinear pairing, where x is a small random integer in $[1, 2^l]$.	0.0535
$T_{bp.a}$	Point addition operation $\bar{P} + \bar{Q}$ related to the bilinear pairing.	0.0071
T_{mtp}	MapToPoint hash operation related to the bilinear pairing.	4.4060
$T_{e.m}$	Scale multiplication operation $a \cdot P$ related to the ECC, where $P \in G$, $a \in Z_q^*$.	0.4420
$T_{e.sm}$	Small scale multiplication operation $x \cdot P$ related to the ECC, where x is a small random integer in $[1, 2^l]$.	0.0138
$T_{e.a}$	Point addition operation $P + Q$ related to the ECC.	0.0018
T_h	General hash function operation $h_k : \{0,1\}^* \rightarrow \{0,1\}^l$.	0.0001

During the whole vehicle message sign phase in ABAH [18], the vehicle requires to conduct two scale multiplication operations and two point addition operations as well as one general hash function operation related to the bilinear pairing, thus, the computation cost of the vehicle is $2T_{bp.m} + 2T_{bp.a} + T_h \approx 3.4323$ ms. For verifying one single message in ABAH [18], the computation of the verifier involves three bilinear pairing operations, one scale multiplication operation, one point addition operation along with one general hash function operation related to the bilinear pairing, namely, the execution time of the verifier is $3T_{bp} + T_{bp.m} + T_{bp.a} + T_h \approx 14.3492$ ms. For batch verifying in ABAH [18] consists of three bilinear pairing operations, (2n) scale multiplication operations, (4n-3) point addition operations as well as (2n) general hash function operations related to the bilinear pairing, consequently, the total computation cost is $3T_{bp} + (2n)T_{bp.m} + (4n-3)T_{bp.a} + (2n)T_h \approx 3.4466n + 12.6117$ ms.

During the whole vehicle message sign phase in the proposed scheme, the vehicle needs to conduct one scale multiplication operation along with one general hash operation related to the ECC, consequently, the computation cost of the vehicle is $T_{e.m} + T_h \approx 0.4421$ ms. The computation cost needed in single verification of one message phase is three scale multiplication operations, two point addition operations and two general hash function operations related to the ECC, accordingly, the execution time of verifying is $3T_{e.m} + 2T_{e.a} + 2T_h \approx 1.3298$ ms. The batch verification of multiple messages phase in the proposed scheme is made up of (n+1) scale multiplication operations, (n) small scale multiplication operations, (n+1) point addition operations and

TABLE IV
COMPARISON ON COMPUTATION COST OF VARIOUS SCHEMES

Scheme	VMS	SVOM	BVMM
ABAH [18]	$2T_{bp.m}+$ $2T_{bp.a}+$ $T_h \approx$ $3.4323ms$	$3T_{bp}+$ $T_{bp.m}+$ $T_{bp.a}+$ $T_h \approx$ $14.3492ms$	$3T_{bp}+$ $(2n)T_{bp.m}+$ $(4n-3)T_{bp.a}$ $+(2n)T_h \approx$ $3.4466n+$ $12.6117ms$
EAAP [22]	$T_{bp.m}+$ $T_h \approx$ $1.7091ms$	$2T_{bp}+$ $5T_{bp.m}+$ $2T_{bp.a} \approx$ $16.9812ms$	$(n+1)T_{bp}+$ $(5n)T_{bp.m}+$ $(2n)T_{bp.a} \approx$ $12.7702n+$ $4.211ms$
EPA-CPPA [23]	$T_{e.m}+$ $2T_h \approx$ $0.4422ms$	$4T_{e.m}+$ $T_{e.a}+2T_h$ $\approx 1.77ms$	$(2n+2)T_{e.m}$ $+(n)T_{e.a}+$ $(2n)T_h \approx$ $0.886n+$ $0.884ms$
PA-CRT [4]	$2T_{e.m}+$ $2T_h \approx$ $0.8842ms$	$3T_{e.m}+$ $2T_{e.a}+1T_h$ $\approx 1.3297ms$	$(n+2)T_{e.m}$ $+(n)T_{e.sm}$ $+(n)T_{e.a}+$ $(2n)T_h \approx$ $0.4578n+$ $0.884ms$
The proposed scheme	$T_{e.m}+$ $T_h \approx$ $0.4421ms$	$3T_{e.m}+$ $2T_{e.a}+2T_h$ $\approx 1.3298ms$	$(n+1)T_{e.m}$ $+(2n)T_{e.sm}$ $+(2n)T_{e.a}$ $+(2n)T_h \approx$ $0.4734n+$ $0.884ms$

VMS: Vehicle Message Signing.
SVOM: Single Verification of One Message.
BVMM: Batch Verification of Multiple Messages.

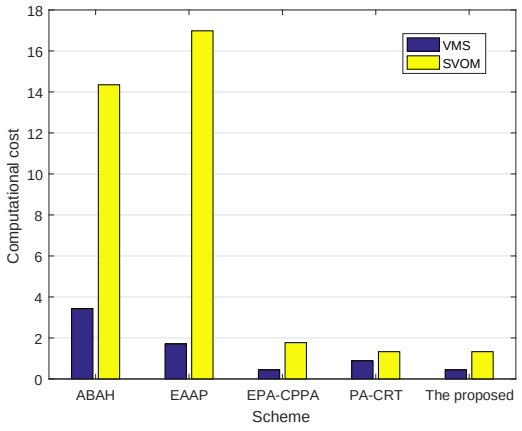


Fig. 5. Comparison of computation cost to sign and verify one message.

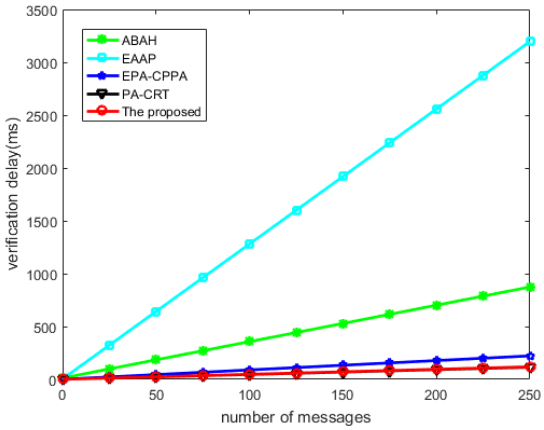


Fig. 6. Comparison on verification delay of batch verification.

(2n) general hash function operations related to the ECC, that is, the total computation cost is $(n+1)T_{e.m}+(2n)T_{e.sm}+(2n)T_{e.a}+(2n)T_h \approx 0.4734n+0.884$ ms.

To more clearly compare the computation cost of between four state-of-art schemes [4], [18], [22], [23] and the proposed scheme, we depict the comparison results from the aspects of computation time on the VMS and the SVOM, as presented in Fig. 5. The results from the Fig. 5 show that our scheme achieves lower computational cost than the four state of-art schemes for vehicular networks.

To prove the major benefit of our scheme in batch verification, we compare the verification delay of batch verification in our scheme with four state-of-art schemes [4], [18], [22], [23], as given in Fig. 6. When the message is 250, the verification delay is observed at 875, 3197, 223, 116 and 120 ms respectively for ABAH [18] scheme, EAAP [22] scheme, EPA-CPPA [23] scheme, PA-CRT [4] scheme and the proposed scheme respectively. Obviously, compared with schemes [18], [22] and [23], the proposed scheme has better performance. Compared with scheme [4], the comparison cost of this scheme is slightly higher, mainly because the ciphertext $S_{i,j} = k_i + h_1(PID_{i,j}, K_{i,j}, TS_j) \cdot s \ mod \ q$ hiding the system private key s contains a random number k_i. The random number k_i corresponding to $\sum_{i=1}^{n} x_i K_{i,j}$ increases the comparison cost of $(n)T_{e.sm}+(n)T_{e.a} = 0.0156n$ ms additionally, i.e. $0.0156 \times 250 \approx 4$ ms. Thus, the proposed scheme gets relatively better performance.

B. Communication Cost Analysis

Here, we compare the communication cost of four state-of-art schemes [4], [18], [22], [23] for vehicular networks. Besides, we consider the sizes of p and $\bar{p}$ are 20 bytes and 64 bytes. Thus, the sizes of those elements in G and G_1 are 40 bytes and 128 bytes, accordingly. Let the timestamps' size be 4 bytes and the hash output of the general hash function be 20 bytes. The comparison result is shown in Table V.

In ABAH [18] scheme, the vehicle broadcasts the message $\langle PID_{i,j}, M_i, tt_i, Y_{i,j} \rangle$, and $Y_{i,j} = (T_{i,j}, U_{i,j}, W_{i,j}) \in G_1$, $PID_{i,j} \in G_1$, tt_i is a timestamp. Thus, the communication cost of the ABAH [18] scheme is $128 \times 4 + 4 = 516$ bytes. In EAAP [22], the vehicle broadcasts the encrypted message $msg = (M||sig||Y_k||Cert_k)$, where $Cert_k = (Y_k||E_i||DID_{\mu_i}||\gamma_U||\gamma_V||c||\lambda||\delta_1||\delta_2)$, $\{Y_k, E_i, DID_{\mu_i}, \gamma_U, \gamma_V\} \in G_1$, $\{\lambda, \delta_1, \delta_2\} \in Z_q^*$, c is the general hash function's output. Namely, the EAAP [22]

TABLE V
COMPARISON ON COMMUNICATION COST OF VARIOUS SCHEMES

Scheme	Sending one message	Sending n messages
ABAH [18]	516 bytes	$516n$ bytes
EAAP [22]	848 bytes	$848n$ bytes
EPA-CPPA [23]	144 bytes	$144n$ bytes
PA-CRT [4]	84 bytes	$84n$ bytes
The proposed scheme	124 bytes	$124n$ bytes

scheme takes $128 \times 6 + 4 \times 20 = 848$ bytes. In EPA-CPPA [23], the vehicle issues the signature message $Msgs = M_i, PID_{i,l}, PK_{i,l}, R_i, T_i, Sig_i$, where $\{PK_{i,l}, R_i, Sig_i\} \in G$, $PID_{i,l} \in Z_q^*$, T_i is a timestamp. Accordingly, the communication cost of the EPA-CPPA [23] is $40 \times 3 + 20 + 4 = 144$ bytes. The PA-CRT [4] takes $40 \times 1 + 20 \times 2 + 4 \times 1 = 84$ bytes for the vehicle sends the message to the verifier communication, where $ID_i = (ID_{i1}, ID_{i2})$, the pseudo identity $ID_{i1} \in G$, $\{ID_{i2}, \sigma_i\} \in {Z_q}^*$ and T_i is a timestamp. In the proposed scheme, $40 \times 2 + 20 \times 2 + 4 = 124$ bytes are expected for the vehicle sends $\{\sigma_i, M_i, T_i, PID_{i,j}\}$ to R_x transmission cost, where the signature includes $\sigma_i = (K_{i,j}, U_{i,j}, \delta_{i,j})$, $\{K_{i,j}, U_{i,j}\} \in G$, $\{\delta_{i,j}, PID_{i,j}\} \in {Z_q}^*$, and T_i is a timestamp. Based on above analysis, the proposed scheme has relatively low communication cost is proved.

In order to highlight the benefits of the proposed scheme, we compare the communication costs for sending a single message of ours with four state-of-art schemes [4], [18], [22], [23] for vehicular networks, as shown in Fig. 7. When the amount of messages reaches 30000 in period of 30s, the bandwidth consumption is observed at 14.76, 24.26, 4.12, 2.4 and 3.55 MB respectively for ABAH [18] scheme, EAAP [22] scheme, EPA-CPPA [23] scheme, PA-CRT [4] scheme and ours respectively. Obviously, compared with schemes [18], [22], [23], the proposed scheme has lower communication overhead. Compared with PA-CRT [4] scheme, the proposed scheme is slightly inadequate. The main reason is that the ciphertext $S_{i,j}$ hiding the master private key s contains the random number k_i. The $K_{i,j}$ corresponding to the random number k_i belongs to the element on G, so compared with scheme [4], the size of 40 bytes is increased by sending a message. In other words, sending n messages takes $40n$ bytes more than PA-CRT [4] scheme, i.e. $40 \times 30000 \approx 1.15$ MB. For the increase in messages' number, the performance of the proposed EABA scheme is relatively better.

C. Average Transmission Delay Comparison

In this subsection, we compare the proposed scheme with the other four schemes [4], [18], [22], [23] on average transmission delay. We use OMNeT++ [45], SUMO [46], Veins [47] and MIRACL [44] to conduct simulation experiments. OMNeT++ is an extensible, modular C++ simulation library and can build network simulators supporting the simulation for wired network and wireless ad-hoc network. SUMO is an open road traffic simulation package designed to handle large road networks. Veins is a middleware to link OMNeT++ and

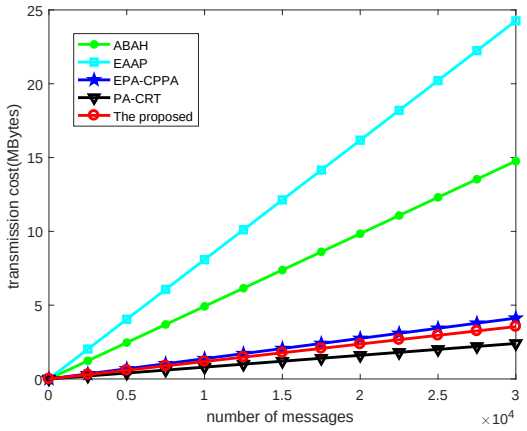


Fig. 7. Comparison on communication cost of various schemes.

TABLE VI
THE PARAMETERS AND VALUES USED

Parameters	Values
Simulation Area	2500×2500 (m^2)
Acceleration speed of vehicle	$10m/s^2$
Data Transmission Rate	24 Mbps
Transmission Power	40 mW
Sensitivity	-89 dBm
Beacon interval	1s
Simulation time	150s

SUMO. The relevant parameters of the simulation experiment are listed in Table VI.

We define the average transmission delay TD of the message between the receiver and the sender in equation (15). $Avg(\cdot)$ refers to a averaging function, n is the number of vehicles, N_i is the number of messages received by V_i. T_r^i, T_s^i represent the time at which the message is sent and the time at which the message is received, respectively.

$$TD = Avg\left(\sum_{j=1}^{n} Avg\left(\sum_{i=1}^{N_i}(T_r^i - T_s^i)\right)\right) \tag{15}$$

Fig. 8 shows the relationship between the average transmission delay and the number of messages when the max speed of vehicles is 15m/s. As we can see from Fig. 8, the scheme proposed in this paper is better than the ABAH [18] scheme and the EAAP [22] scheme, and a little better than the PA-CRT [4] scheme in most cases. The relationship between the average transmission delay and the speed of vehicles when the fixed size of packages sent by vehicles is 400 KB is shown in Fig. 9. With reference to the vehicular applications' requirements in reachability and latency in Table II, the delay satisfies the latency requirement ($\leq$ 20 ms) by the vehicle safety applications that require vehicle-to-vehicle broadcasting. According to Fig. 9 and Table II, we can draw a conclusion that the proposed scheme is superior to other schemes in the matter of average transmission delay and can meet the latency requirement of the vehicular network.

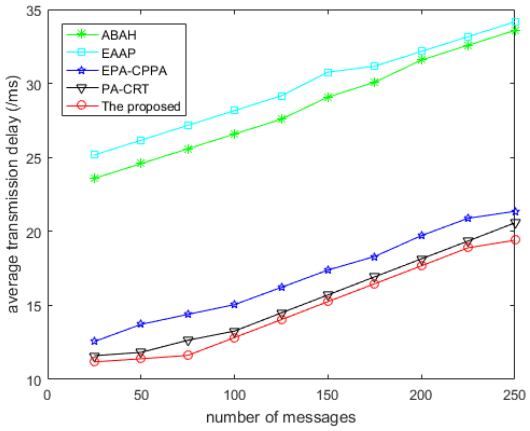


Fig. 8. Simulation results in average transmission delay with number of messages.

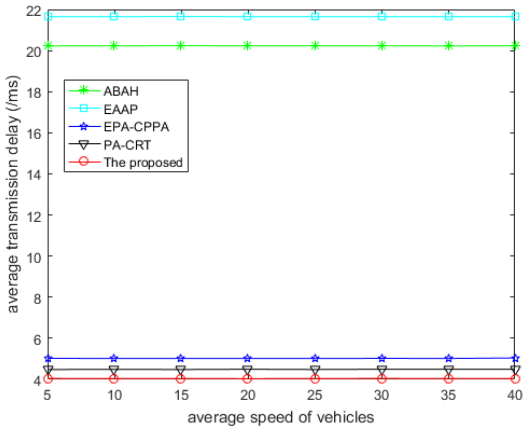


Fig. 9. Simulation results in average transmission delay with average speed of vehicles.

VI. Conclusion

We proposed an extensible and effective anonymous batch authentication (EABA) scheme. The EABA can effectively avoid side channel attacks, not only meeting security and privacy requirements, but also reducing computational and transmission overhead to a certain extent. Moreover, the TA only needs to release two hash seeds to revoke illegal vehicles. We also proposed a method for rapid distributing CRLs, effectively preventing attackers from taking false messages with unexpired certificates. For our future work, we will study how vehicles can establish their own groups for secure communication and how to protect vehicles' location privacy without the help of infrastructure.

VII. Acknowledgment

The work was supported by the National Natural Science Foundation of China (No.61872001, No.61702005), the Key Program of National Natural Science Foundation of China (No. U1936220), the Open Fund of Key Laboratory of Embedded System and Service Computing (Tongji University), Ministry of Education (No. ESSCKF2018-03), the Open Fund for Discipline Construction, Institute of Physical Science and Information Technology, Anhui University and the Excellent Talent Project of Anhui University. The authors are very grateful to the anonymous referees for their detailed comments and suggestions regarding this paper.

References

[1] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2017.

[2] A. Gilchrist, *Industry 4.0: the industrial internet of things*. Apress, 2016.

[3] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (vanets): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[4] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "Pa-crt: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Transactions on Dependable and Secure Computing*, 2019.

[5] J. B. Kenney, "Dedicated short-range communications (dsrc) standards in the united states," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[6] T. S. Abraham and K. Narayanan, "Cooperative communication for vehicular networks," in *2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies*. IEEE, 2014, pp. 1163–1167.

[7] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[8] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in internet of vehicles: A review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 5, pp. 2339–2352, 2015.

[9] Y.-W. Lin, Y.-S. Chen, and S.-L. Lee, "Routing protocols in vehicular ad hoc networks: A survey and future perspectives." *J. Inf. Sci. Eng.*, vol. 26, no. 3, pp. 913–932, 2010.

[10] S. M. Pournaghi, B. Zahednejad, M. Bayat, and Y. Farjami, "Necppa: A novel and efficient conditional privacy-preserving authentication scheme for vanet," *Computer Networks*, vol. 134, pp. 78–92, 2018.

[11] A.-S. K. Pathan, *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2016.

[12] C.-C. Hung, H. Chan, and E. H.-K. Wu, "Mobility pattern aware routing for heterogeneous vehicular networks," in *2008 IEEE Wireless Communications and Networking Conference*. IEEE, 2008, pp. 2200–2205.

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

[14] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.

[15] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*. IEEE, 2015, pp. 1–6.

[16] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3589–3603, 2010.

[17] H. Lu and J. Li, "Privacy-preserving authentication schemes for vehicular ad hoc networks: a survey," *Wireless Communications and Mobile Computing*, vol. 16, no. 6, pp. 643–655, 2016.

[18] S. Jiang, X. Zhu, and L. 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.

[19] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "Spacf: A secure privacy-preserving authentication scheme for vanet with cuckoo filter," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10 283–10 295, 2017.

[20] A. A. Rasheed, R. N. Mahapatra, and F. G. Hamza-Lup, "Adaptive group-based zero knowledge proof-authentication protocol in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, 2019.

[21] J. Cui, D. Wu, J. Zhang, Y. Xu, and H. Zhong, "An efficient authentication scheme based on semi-trusted authority in vanets," *IEEE Transactions on Vehicular Technology*, 2019.

[22] M. Azees, P. Vijayakumar, and L. J. Deboarh, "Eaap: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[23] J. Li, K.-K. R. Choo, W. Zhang, S. Kumari, J. J. Rodrigues, M. K. Khan, and D. Hogrefe, "Epa-cppa: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *Vehicular Communications*, vol. 13, pp. 104–113, 2018.

[24] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, "Rsma: Reputation system-based lightweight message authentication framework and protocol for 5g-enabled vehicular networks," *IEEE Internet of Things Journal*, 2019.

[25] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 2, pp. 907–919, 2013.

[26] S. Tangade, S. S. Manvi, and P. Lorenz, "Decentralized and scalable privacy-preserving authentication scheme in vanets," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8647–8655, 2018.

[27] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1557–1568, 2007.

[28] Y. Zhang, L. Yang, and S. Wang, "An efficient identity-based signature scheme for vehicular communications," in *2015 11th International Conference on Computational Intelligence and Security (CIS)*. IEEE, 2015, pp. 326–330.

[29] C. Gañán, J. L. Muñoz, O. Esparza, J. Mata-Díaz, and J. Alins, "Epa: an efficient and privacy-aware revocation mechanism for vehicular ad hoc networks," *Pervasive and Mobile Computing*, vol. 21, pp. 75–91, 2015.

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

[31] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications," in *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*. IEEE, 2008, pp. 1229–1237.

[32] A. Wasef, Y. Jiang, and X. Shen, "Ecmv: efficient certificate management scheme for vehicular networks," in *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*. IEEE, 2008, pp. 1–5.

[33] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in vanets," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3235–3248, 2017.

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

[35] T. W. Chim, S.-M. Yiu, L. C. Hui, and V. O. Li, "Specs: Secure and privacy enhancing communications schemes for vanets," *Ad Hoc Networks*, vol. 9, no. 2, pp. 189–203, 2011.

[36] W. I. Khedr, "Improved lightweight authentication scheme for ieee 802.11 p vehicle-to-infrastructure communication." *Adhoc & Sensor Wireless Networks*, vol. 31, 2016.

[37] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1319–1328, 2015.

[38] W. Mao, *Modern cryptography: theory and practice*. Pearson Education India, 2003.

[39] C.-P. Schnorr, "Efficient signature generation by smart cards," *Journal of cryptology*, vol. 4, no. 3, pp. 161–174, 1991.

[40] S.-J. Horng, S.-F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, and M. K. Khan, "b-specs+: Batch verification for secure pseudonymous authentication in vanet," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1860–1875, 2013.

[41] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of cryptology*, vol. 13, no. 3, pp. 361–396, 2000.

[42] Z. Xu, X. Li, X. Zhao, M. H. Zhang, and Z. Wang, "Dsrc versus 4g-lte for connected vehicle applications: A study on field experiments of vehicular communication performance," *Journal of Advanced Transportation*, vol. 2017, 2017.

[43] R. Chen, D. Ma, and A. Regan, "Tari: Meeting delay requirements in vanets with efficient authentication and revocation," in *2nd International Conference on Wireless Access in Vehicular Environments (WAVE)*, 2009.

[44] E. Wenger and M. Werner, "Evaluating 16-bit processors for elliptic curve cryptography," in *International Conference on Smart Card Research and Advanced Applications*. Springer, 2011, pp. 166–181.

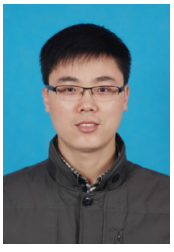
[45] A. Varga, "Discrete event simulation system," in *Proc. of the European Simulation Multiconference (ESM2001)*, 2001, pp. 1–7.

[46] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "Sumo–simulation of urban mobility: an overview," in *Proceedings of SIMUL 2011, The Third International Conference on Advances in System Simulation*. ThinkMind, 2011.

[47] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved ivc analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, 2010.

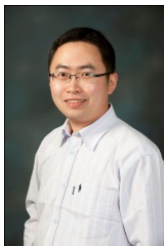
Jing Zhang is currently a PhD student in the School of Computer Science and Technology, Anhui University, Hefei, China. Her research interests include vehicular ad hoc network, IoT security and applied cryptography. She has over 10 scientific publications in reputable journals (e.g. IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Vehicular Technology, IEEE Transactions on Intelligent Transportation Systems, Information Sciences, Science China Information Sciences and Vehicular Communications) and international conferences.

Hong Zhong was born in Anhui Province, China, in 1965. She received her PhD degree in computer science from University of Science and Technology of China in 2005. She is currently a professor and Ph.D. supervisor of the School of Computer Science and Technology at Anhui University. Her research interests include applied cryptography, IoT security, vehicular ad hoc network, cloud computing security and software-defined networking (SDN). She has over 120 scientific publications in reputable journals (e.g. IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Vehicular Technology, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Network and Service Management, IEEE Transactions on Big Data and IEEE Internet of Things Journal), academic books and international conferences.



Jie Cui was born in Henan Province, China, in 1980. He received his Ph.D. degree in University of Science and Technology of China in 2012. He is currently an associate professor and Ph.D. supervisor of the School of Computer Science and Technology at Anhui University. His current research interests include applied cryptography, IoT security, vehicular ad hoc network, cloud computing security and software-defined networking (SDN). He has over 80 scientific publications in reputable journals (e.g. IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Vehicular Technology, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Network and Service Management, IEEE Transactions on Emerging Topics in Computing, IEEE Transactions on Circuits and Systems and IEEE Internet of Things Journal), academic books and international conferences.

Yan Xu is an associate professor in the School of Computer Science and Technology, Anhui University. She received Ph.D. degree in University of Science and Technology of China in 2015. Her research interests include network and information security.



Lu Liu is the Professor of Informatics and Head of Department of Informatics in the University of Leicester, UK. Prof Liu received the Ph.D. degree from University of Surrey, UK and MSc in Data Communication Systems from Brunel University, UK. Prof Liu's research interests are in areas of cloud computing, service computing, computer networks and peer-to-peer networking. He is a Fellow of British Computer Society (BCS).