IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 21, 2019, accepted April 2, 2019, date of current version May 6, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2911924

An Efficient Privacy-Preserving Mutual Authentication Scheme for Secure V2V Communication in Vehicular Ad Hoc Network

LIBING WU[1,2], QIANQIAN SUN[1], XINPEI WANG[1], JING WANG[1], SHUI YU[3], YIFEI ZOU[4], BINGYI LIU[2], AND ZIKE ZHU[5]

[1]School of Computer Science, Wuhan University, Wuhan 430072, China
[2]Hubei Key Laboratory of Transportation Internet of Things, Wuhan University of Technology, Wuhan 430072, China
[3]School of Software, University of Technology Sydney, Ultimo, NSW 2007, Australia
[4]Deparment of Computer Science, The Chinese University of Hong Kong, Hong Kong
[5]School of Economics and Finance, Wuhan University of Technology, Wuhan 430072, China

Corresponding author: Libing Wu (wu@whu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61772377, Grant 61572370, and Grant 91746206, in part by the Natural Science Foundation of Hubei Province of China under Grant 2017CFA007, in part by the Science and Technology Planning Project of ShenZhen under Grant JCYJ20170818112550194, and in part by the Fund of Hubei Key Laboratory of Transportation Internet of Things under Grant WHUTIOT-2017A0011.

ABSTRACT Recent years have witnessed that the new mobility Intelligent Transportation System is booming, especially the development of Vehicular Ad Hoc Networks (VANETs). It brings convenience and a good experience for drivers. Unfortunately, VANETs are suffering from potential security and privacy issues due to the inherent openness of VANETs. In the past few years, to address security and privacy-preserving problems, many identity-based privacy-preserving authentication schemes have been proposed by researchers. However, we found that these schemes fail to meet the requirements of user privacy protection and are vulnerable to attacks or have high computational complexity. Hence, we focus on enhancing privacy-preserving via authentication and achieving better performance. In this paper, first, we describe the vulnerabilities of the previous scheme. Furthermore, to enhance privacy protection and achieve better performance, we propose an efficient privacy-preserving mutual authentication protocol for secure V2V communication in VANETs. Through security analysis and comparison, we formally demonstrate that our scheme can accomplish security goals under dynamic topographical scenario compared with the previous scheme. Finally, the efficiency of the scheme is showed by performance evaluation. The results of our proposed scheme are computationally efficient compared with the previously proposed privacy-preserving authentication scheme.

INDEX TERMS VANETs, authentication, V2V, privacy-preserving, security, identity guessing attack.

I. INTRODUCTION

In recent years, along with the fast growth of intelligent transportation systems (ITSs) [1] and wireless technologies (e.g., GPRS, VLC, 5G, WiMAX and GSM), Vehicular Ad Hoc Networks (VANETs) [2] become increasingly prosperous, enabling mobile devices to enjoy convenient and comprehensive services. As [3] pointed out, in the Internet of things, there are different forms in different application fields, such as VANETs. Vehicles as mobile devices are generally equipped with sensors (e.g., speed, acceleration, position, rotational speed sensor), processors and wireless communication equipment (e.g., Bluetooth, Wi-Fi, OBU) to perform all terminal perception, computation and communication tasks [4]. Vehicles can communicate and share information with each other, since VANET is a mobile wireless network [5]. It is envisaged that the police may demand to require information from drivers, but drivers may pay close attention to their own personal sensitive information (e.g., identity, location history and movements) when they

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

communicate in the VANETs environment which exists security threats. It is possible that these valuable data may be stolen by the adversary in the above communication process. That's why mobile users, researchers even governments pay greater attention to security issues to achieve better implement of real-time and intelligent applications [6].

There are two different communication scenarios, namely Vehicle To Infrastructure (V2I) and Vehicle To Vehicle (V2V) in VANETs. As shown in Figure 1, there are three major units in VANETs, which are the authentication server (AS), wireless onboard unit (OBU) and roadside unit (RSU). Vehicles in VANETs are deemed as mobile nodes equipped with OBUs with an integration of the GPS receiver, ITS-G5/IEEE 802.11p protocols, and vehicular sensors [7]. The OBU is in charge of recording information (e.g., velocity, location) during driving and allows itself to correspond with RSU or other vehicles. The RSU is fixed at the roadsides and plays itself as public transport infrastructure to connect the vehicle to the Internet through reliable communication channels. Further, because of equipping with wireless devices, RSU can exchange information with passing vehicles and gather information to know about local situations [8]. Due to above features and their inherent openness, VANETs are facing a serious security challenge, like the issues of information confidentiality, information integrity. Hence, it is becoming increasingly important for protocols to have the ability to provide drivers with secure and user friendly authentication to achieve a secure communication [9].

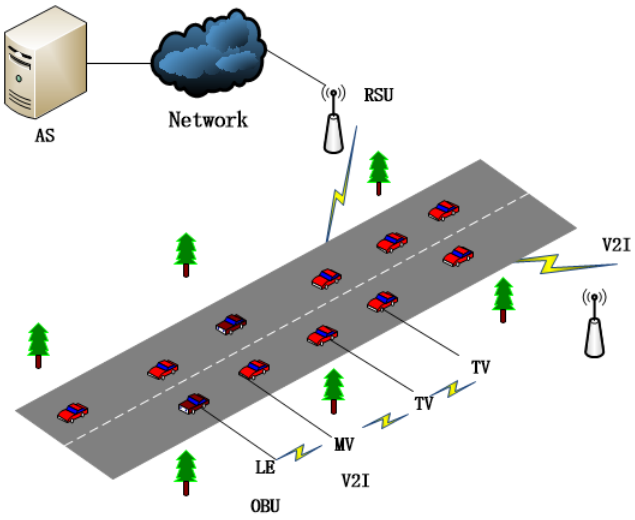


FIGURE 1. Structure of the VANETS.

Owing to VANETs are vulnerable to malicious attacks just as any other wireless network [7], [10]–[14], more and more researchers are having eye on and taking part in privacy protection authentication. Authentication protocols for VANETs have been designed by most researchers, including those put forward for offering privacy protection during the period of communication and those proposed for a reduction of the storage and computation/communication costs. However, existing authentication protocols generally have shortcomings against the external adversary. VANETs still need a secure and effective authentication scheme. Our research aims to construct an efficient and secure authentication scheme to eliminate these vulnerabilities of Zhou et al.'s scheme under VANETs environment.

The major contributions of our improved scheme are listed as following:

A. OUR CONTRIBUTIONS

- First, in order to enhance the security, we bring up an efficient privacy protection mutual authentication protocol for secure V2V communication in VANETs to overcome the shortcomings of Zhou et al.'s scheme.
- Second, we reveal the weakness of Zhou et al.'s scheme and give an in-depth description of the damaging threat of the existing weakness.
- Third, we present an elaborate security analysis to formally demonstrate that the proposed scheme is provable security and meet the security goals in VANETs, especially in key protection.
- Finally, we display our performance analysis to demonstrate that our scheme has a reasonable consumption with a lower computation and communication cost than the previous scheme in VANETs.

B. ROADMAP

To present our contributions and work, the rest of the framework for this paper is structured as follows. The related work in recent years is introduced in section II. We present the preliminaries to the elliptical curve cryptosystem in Section III. In Section IV, we have a review of Zhou et al.'s scheme. In addition, section V points out its existing security vulnerabilities. The main improvement of our proposal is described in Section VI while Section VII describes the security analysis. We show the performance evaluation to demonstrate our scheme's reasonable overhead in Section VIII. At last, we provide the conclusion of the paper in last section.

II. RELATED WORK

In order to address security and privacy issue in VANETs, numerous research schemes [15]–[26], [30]–[32] have been proposed. Raya and Hubaux [15] investigated an authentication scheme which pre-storaged many public and private key pairs with a short lifecycle, as well as corresponding certificates into each vehicle's OBU to preserve drivers' privacy. However, a vehicle's OBU needs to store very large number key pairs due to the changing key each time. Raya and Hubaux's scheme has a high computation cost, since the key management is a complex problem.

To solve the shortcomings of Raya and Hubaux scheme, a new privacy protection protocol, which adopted an alternative approach to avoidance of the preloading of a large number of public or private key pairs of OBU and corresponding certificates was designed by Lu et al. [17] in 2008. In their scheme, when a vehicle passes through the RSU,

each vehicle will receive an anonymous certificate for a short period of time. In order to obtain anonymous certificates that change over time from RSU to avoid the adversary's traceability, the vehicle needs to execute this procedure frequently. Hence, Lu et al.'s scheme with high computation/communication and storage costs has a weak efficiency. To address the weakness of Lu et al.'s scheme, a novel authentication protocol combining mix-zones with anonymous certificates was proposed by Freudiger et al. [18]. However, the scheme also must store massive anonymous certificates. Additionally, in 2008, Zhang et al. [19] designed a privacy-preserving authentication protocol with the Hash message authentication code in VANETs. In their scheme, for the sake of user's privacy, the vehicle communicates with near RSU using different public keys. Therefore, Zhang et al.'s scheme also fails to meet the requirement of performance in VANETs.

To address high computation and high storage costs problems, these schemes [25], [26], [30]–[32] were proposed. Zhang et al. [24], [25] designed an ID-based conditional privacy protection authentication scheme in VANETs. In their scheme, both the vehicle and RSU are not necessary to store certificates. However, Lee and Lai found that [24], [25] cannot resist replying attacks. [31] designed a conditional privacy protection authentication and group-key agreement scheme based on password for VANETs with no use bilinear pairing. References [30], [32] proposed a privacy-preserving authentication scheme to improve computation efficiency. Chuang and Lee [26] proposed the first authentication mechanism (TEAM) using a transitive trust relationship for VANETs in 2014. TEAM is a quite lightweight privacy-preserving authentication scheme, since it only uses a hash function and an XOR operation to protect the drivers' privacy and security from malicious adversary. Vehicles are divided into three types in their scheme, that is, mistrustful vehicles (MVs), trustful vehicles (TVs) and law executors (LEs), as shown in Figure 1. However, Kumari et al. [5] and Zhou et al. [23] revealed that Chuang and Lee's scheme suffers from privacy breach, insider attack, impersonation attack and has some other weaknesses. To address these vulnerabilities, on the basis of TEAM, Zhou et al. applied Elliptic Curve Cryptographic (ECC) to propose a new enhanced scheme which is based on mutual authentication in VANETs. Nevertheless, according to our research efforts, Zhou et al.'s scheme cannot withstand identity guessing attack and impersonation attack as well as has weaker user anonymity.

To enhance security and privacy protection in VANETs, we also use ECC technology to design a new privacy-preserving authentication scheme. The formal and informal security analysis of our proposed scheme indicates its provable security and could overcome the vulnerability in Zhou et al.'s scheme. The performance analysis of our proposed scheme demonstrates that it yields lower computational and communication overheads making it applicable to dynamic topographic scenarios.

III. PRELIMINARIES

Mathematical problems in Elliptic Curve Cryptographic have been widely used in the authentication scheme in VANETs. In this paper, our proposed scheme uses the problem of elliptic curve discrete logarithm to achieve its security. The brief reviews on ECC are as follows:

Let G be an elliptic curve group, which is defined by a prime number p and a generator P. The following two difficult problem assumptions are based on ECC and these problems are difficult to solve.

Let E be an equation of the elliptic curve: $y = x^3 + ax + b \bmod p$, where $a, b \in_R Z_p^*$.

Definition 1: Discrete Logarithm Problem (DLP): Given two points P and Q on E randomly, the objective of the DLP is to calculate an integer $a \in_R Z_p^*$ to meet the following condition: Q is equal to aP.

Definition 2: Elliptic Curve Computational Diffe-Hellman Problem (ECCDHP): Given two points $R = aP$ and $Q = bP$ on E randomly, the objective of the ECCDHP is to calculate the point abP, where $a, b \in_R Z_p^*$ are two unknown integers.

IV. REVIEW OF THE ZHOU ET AL.'s SCHEME

We review the Zhou et al.'s scheme based on TEAM for VANETs in this section. TABLE 1 shows the symbols and their corresponding meanings. We are only keen on six phases of this scheme: initialization, registration, login, general authentication, secure communication, key update. In their scheme, as shown in Figure 1, vehicles have three types: first is law executors (LEs), second is trustful vehicles (TVs) and third is mistrustful vehicles (MVs). LEs are always trustful and play a role of mobile authentication server. In the beginning, the normal vehicle is authenticated only via LE. Later, if this normal vehicle is successfully authenticated, it will become a trustful vehicle.

TABLE 1. The notations and specific descriptions.

Notations	meanings
AS	an honest party (Authentication Server)
OBU	On Board Unit
RSU	Roadside Unit
LE	Law Executor
TV	Trustful Vehicle
MV	Mistrustful Vehicle
x	the AS's secret key
x_i	OBU_i's secret key
psk	the pre-shared key between LE and AS
$User_i$	the ith user
id_i	the identity of the ith user
pw_i	the password of the the ith user
h	the hash function
sk_{ij}	the session key between the i and j
$\|\|$	the connection symbol
$\oplus$	the XOR operator
msg_{kup}	the message of key update

Otherwise, it still a mistrustful vehicle. At this time, a normal vehicle can be authenticated by LE or a trustful vehicle. When the key's lifecycle expires, the vehicle's state changes from trust to mistrust.

The whole process consists of 9 phases, which are initialization, registration, login, password change, general authentication, trust-extended authentication, secure communication, key revocation, and key update. When AS starts to set up the system parameters, the initiation phase will be performed. Registration has two types, namely LE registration and normal vehicle registration. In LE registration phase, a LE registers itself as a trustful vehicle with AS using a secure transmit channel. In normal vehicle registration phase, which is performed only once by per vehicle, all vehicles but LEs have to execute this phase before they enter into VANETs. $User_i$ has to execute the login phase, when it hopes to VANETs supply the best service for it. And if the $User_i$ wants to try changing its password, the password change process is started. After $User_i$ has completed its login phase, the general authentication procedure is performed between OBU_i and LE_j. At this time, the state of OBU_i changes from mistrust to trust and gets the parameter psk (i.e., authentication key) after achieving the general authentication procedure successfully. Mistrustful OBUs can get authenticated by LEs at the general authentication phase or trusted OBU_i in trust-extended authentication phase at present. Then, two trustful vehicles can have a communication at secure communication phase. When the key's lifecycle expires, the vehicle's state will become mistrustful and the key revocation will be performed. The state of the OBU_i continues to be mistrustful again when the lifecycle of key expires, and the key revocation will be performed. When the key of a trustful vehicle is nearing expiration, it can update the key during the key update phase. This is the whole process of Zhou et al.'s scheme.

Each vehicle is equipped with the OBU consisting of Event Data Recorders (EDRs) and Tamper-Proof Devices (TPDs). The former are in charge of recording event data (e.g., time, location, login history of the vehicle, public parameters). The latter prevent attackers from intercepting information from OBU. Additionally, assuming that the GPS device synchronizes the time of each vehicle. The vehicle broadcasts the message with the authentication state (trusted or mistrusted) periodically. The following displays Zhou et al.'s scheme in detail.

A. INITIALIZATION

The following two steps are initialization procedures for AS when setting up system parameters.

1) Let G be an elliptic curve group, which is defined by a prime number p and a generator P.
2) The AS chooses x at random from ${}_RZ_p^*$ as its secret key and uses the one way hash chain method to calculate secure key-sets $\{ psk_i, i = 1, \ldots, n \}$, such as, $h^2(x) = h(h(x))$, which is showed in Figure 2.

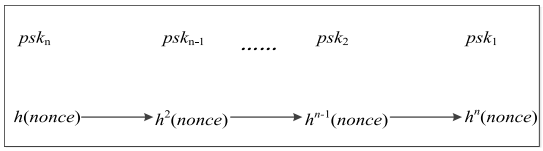


FIGURE 2. Generating key set by Hash Chain method.

B. REGISTRATION

1) LE REGISTRATION

LE is registered with AS through a secure channel in this process. AS uses the hash-chain to calculate secure key-sets $\{ psk_i, i = 1, \ldots, n \}$, and sends both key-sets and public parameters $\{ G, P, p \}$ to LE. LE stores these parameters in its reliable security hardware OBU. To ensure the robust security, the lifecycle of every psk_i needs to be set shorter.

2) NORMAL VEHICLE REGISTRATION

When all vehicles enter the market, they are required to perform the procedure by means of the manufacturer or a secure channel, but LE is an exception. Each vehicle is registered only once in this process. Here are several steps of this stage:

1) $User_i \rightarrow$ AS: $User_i$ selects its password pw_i, then transmits its identity id_i and pw_i to the AS using a secure channel.
2) After receiving the identity id_i and secret password pw_i from $User_i$, the AS selects y_i as a random number, and then calculates $a_i = h(x||id_i)$, $b_i = a_i \oplus h(pw_i)$, $c_i = a_i \oplus h(psk||y_i)$, $d_i = h(id_i||pw_i||a_i)$.
3) AS $\rightarrow User_i$: The AS stores the parameters (i.e., $h()$, G, P, p, b_i, c_i, d_i, y_i) in its OBU reliable security hardware using a secure channel.
4) $User_i$ selects a number x_i as its private key, and then calculates $P_{pub_i} = x_iP$ which is deemed to its public key, and then calculates $z_i = h(pw_i) \oplus x_i$ and stores both P_{pub_i} and z_i in its reliable security hardware.

C. LOGIN

When a $User_i$ intends to access service from VANETs, this procedure is performed.

1) $User_i \rightarrow OBU_i$: $User_i$ submits its real identity id_i and password pw_i to OBU_i.
2) Verify: OBU_i recalculates $a_i = h(pw_i) \oplus b_i$. Then it verifies $d_i = h(id_i||pw_i||a_i)$ holds or not. If so, it indicates that these parameters (id_i, pw_i) inputted by the $User_i$ are correct. Otherwise, OBU_i denies the user login request.

D. GENERAL AUTHENTICATION

On completing the login process, OBU_i implements this procedure with the help of the LE. Here are seven steps of this stage.

1) The OBU_i calculates $aid_i = h(r_i) \oplus id_i$, where $r_i \in {}_RZ_p^*$ is generated randomly, $m_1 = h(a_i) \oplus r_i$ and $m_2 = h(r_i||aid_i||c_i||y_i)$, where a_i is obtained from login phase.

2) $OBU_i \rightarrow LE_j$: OBU_i obtains these parameters (i.e., aid_i, c_i, y_i, m_1, m_2) after step 1), and then it sends these authentication parameters to LE_j.
3) LE_j receives these authentication parameters (i.e., aid_i, c_i, y_i, m_1, m_2) after step 2) from OBU_i, and then it uses psk to recalculate a_i and $r_i = m_1 \oplus h(a_i)$ and then verifies whether $m_2 = h(r_i||aid_i||c_i||y_i)$ holds or not. If so, LE_j calculates $aid_j = id_j \oplus h(r_j)$, where $r_j \in_R Z_p^*$, $sk_{ij} = h(r_i||r_j)$. Then LE_j computers the reply message $m_3 = r_j \oplus h^2(r_i)$, $m_4 = psk \oplus r_j$, and the verification message $m_5 = h(aid_j||sk_{ij}||r_j||psk)$.
4) $LE_j \rightarrow OBU_i$: On calculating these response messages, LE_j returns response messages (i.e., m_3, m_4, m_5, aid_j) to OBU_i.
5) receiving the response message after step 4) from LE_j, OBU_i calculates $h^2(r_i)$ and then retrieves $r_j = m_3 \oplus h^2(r_i)$, and then uses r_j to retrieve $psk = r_j \oplus m_4$, and $sk_{ij} = h(r_i||r_j)$. Next, OBU_i computers $h(aid_i||sk_{ij}||r_j||psk)$ and checks if it and m_5 are equal. If not so, the OBU_i terminates the process. Otherwise, OBU_i computers the $m_6 = sk_{ij} \oplus h(r_j)$ and then calculates: $c_i^* = h(psk||r_i) \oplus a_i$, $e_i = psk \oplus h(pw_i)$. At this time, c_i^* and r_i take place of c_i and y_i. Finally, OBU_i stores them in its reliable security hardware.
6) $OBU_i \rightarrow LE_j$: OBU_i sends m_6 to LE_j.
7) LE_j calculates $h(r_j)$, where r_j is generated at step 3) and uses sk_{ij} to retrieve $h(r_j)$ and checks whether the two have value are equal.

At this time, OBU_i is trustful since it has obtained the authentication parameter psk. From now to start, OBU_i can authenticate other normal vehicles like LE.

E. SECURE COMMUNICATION

When two trusted OBU_i and OBU_j intend to have an interaction with each other, they will perform the secure communication procedure, the followings are the steps.

1) OBU_i uses e_i to retrieve $psk = e_i \oplus h(pw_i)$ and uses z_i to retrieve $x_i = z_i \oplus h(pw_i)$ and calculates the message $aid_i = id_i \oplus h(r_i P_{pub_j})$, where r_i is generated randomly, $T = r_i P$, $u_i = T + psk \cdot P$, and $m_1 = h(T||id_i||aid_i)$.
2) $OBU_i \rightarrow OBU_j$: The request information (i.e., m_1, aid_i, u_i) is transmitted to OBU_j by OBU_i.
3) As soon as OBU_j receives these secure communication messages (i.e., m_1, aid_i, u_i) from OBU_i, it uses psk to retrieve $T = u_i$ - psk, and then calculates $id_i = aid_i \oplus h(x_j T)$, and checks if m_1 and $h(T||id_i||aid_i)$ are equal. If not, the request will be rejected. Otherwise, OBU_j generates a random number r_j and calculates: $aid_j = id_j \oplus h(r_j P_{pub_i})$, $R = r_j P$, $u_j = R + psk \cdot P$, $s = r_j P_{pub_i} + x_j T$, $k = h(T||R||P_{pub_i}||P_{pub_j}||s)$, $m_2 = h(id_j||k)$.
4) $OBU_j \rightarrow OBU_i$: OBU_j sends the response information (i.e., aid_j, m_2, u_j) to OBU_i.
5) Upon receiving (i.e., aid_j, u_j) from OBU_j, OBU_i calculates $R = u_j$ - $psk \cdot P$, $id_j = aid_j \oplus h(x_i R)$, $s = r_i P_{pub_j} + x_i R$, $k = h(T||R||P_{pub_i}||P_{pub_j}||s)$, then checks whether m_2 and $h(id_j||k)$ are equal. If yes, OBU_i believes OBU_j is trustful and calculates the reply information $m_3 = h(u_j||k)$. If not, the process will be terminated.
6) $OBU_i \rightarrow OBU_j$: OBU_i sends m_3 to OBU_j.
7) Upon receiving m_3 from OBU_i, OBU_j checks whether m_3 and $h(u_j||k)$ are equal. If yes, the session key k can be used for secure communication. If not, the process will be terminated.

F. KEY UPDATE

In Zhou et al.'s scheme, the procedure is as same as in the Chuang-Lee scheme.

V. WEAKNESS OF ZHOU ET AL.'s SCHEME

In this section, we show that Zhou et al.'s scheme fails to withstand the identity guessing and the impersonation attack even the session key leaking. In particular, it cannot achieve the security requirement of resisting the identity guessing in Zhou et al.'s scheme.

A. IDENTITY GUESSING ATTACK

Here, we list the steps that the adversary guesses the user's identity.

1) Guess the value of id_i to be id_i^* from a uniformly distributed identity dictionary D_{id}.
2) Precisely because the open channel is exposed and unprotected on VANETs, the adversary can intercept some messages as follows: $\{aid_i, m_1, m_3, m_4, c_i, y_i\}$.
3) Calculate $h^*(r_i) = aid_i \oplus id_i^*$, $r_j^* = m_3 \oplus [h^*(r_i)]^2$, $psk^* = r_j^* \oplus m_4$, $a_i^* = h(psk^*||y_i) \oplus c_i$, $r_i^* = m_1 \oplus h(a_i^*)$, $sk_{ij} = h(r_i^*||r_j^*)$, where $\{aid_i, m_1, m_3, m_4, c_i, y_i\}$ is intercepted from the public channel.
4) Verify the correctness of id_i^* by comparing $h(r_i^*)$ and $h^*(r_i)$ holds or not.
5) Repeat 1), 3), 4) until the correct value of id_i is found.

Let $|D_{id}|$ be the size of the identity dictionary D_{id}. As a matter of fact, $|D_{id}|$ is limited for users' own reasons. It is well known that users are prone to choose identities that are easier to remember for convenience, or a meaningful phrase as his/her identity in normal circumstances. Bonneau and Joseph [27] pointed out that the space of D_{id} has a range, e.g., $|D_{id}| \leq |D_{pw}| \leq 10^6$. Moreover, the procedure of the identity guessing for the adversary only requires passive guessing attack and does not involve special encryption operations. And the time complexity of the above attack procedure is $O(|D_{id}| * T_H)$, where T_H is the execution time of the Hash function. That's to say, the time for the adversary to obtain the OBU_i's identity is a linear function of the $|D_{id}|$. According to the above description, identity guessing attack is very effective for the adversary.

Assuming the correct value of id_i is obtained by the adversary, user's real identity will be found. Therefore, identity guessing attack helps the adversary reveal the user's real identity id_i. Hence, Zhou et al.'s scheme is vulnerable to identity guessing attack and provides weaker user anonymity.

B. SECURE SESSION KEY DISCLOSURE

As we all know, it is important that principals can prove each other's identities to realize identity authentication and then build a session key for a secure networked authentication system. The session key sk_{ij} created between OBU_i and LE_j in the process of general mutual authentication can be extracted by the adversary through $sk_{ij} = h(r_i^*||r_j^*)$, where r_i^* and r_j^* are obtained from identity guessing attack phase. If the adversary finds the correct value of id_i, the session key will be disclosed.

C. IMPERSONATION ATTACK

To impersonate as OBU_i, the adversary should be able to access the user's associated value r_i, otherwise he/she cannot obtain the valid authentication request message. For the adversary can select the random number r_i^*, which can also be recovered from the procedure of identity guessing attack, and obtain aid_i, c_i, y_i from the open channel on the Internet, and he/she can compute the correct request message $m_2 = h(r_i^*||aid_i||c_i||y_i)$. Hence, [23] cannot resist an impersonation attack.

In above analysis, we have revealed that the scheme proposed by Zhou et al could not achieve certain important security requirements in our new but realistic attacking scenario.

VI. THE PROPOSED IMPROVED SCHEME

This section proposes an improved privacy protection authentication scheme to address these shortcomings of Zhou et al.'s scheme [23] in VANETs. There are also three types of vehicles in our proposed scheme, which are law executors (LEs), trusted vehicles (TVs) and mistrusted vehicles (MVs) respectively, as shown in Figure 1. There are also nine phases in our proposed scheme: Initialization, Registration, Login, Password Change, General Authentication, Trust-Extended Authentication, Secure Communication, Key Revocation, Key Update. Table 1 shows all notations used in our scheme. In the following, we describe our proposed improved scheme in depth.

A. INITIALIZATION

This procedure mainly is used by the AS to set up the system parameters and it is as same as in Zhou et al.'s scheme.

B. REGISTRATION

1) LE REGISTRATION

This procedure is as same as in Zhou et al.'s scheme.

2) NORMAL VEHICLE REGISTRATION

Except for LE does not require this registration, all other vehicles have to be registered in this phase when they left the car factory. Each vehicle is registered only once in this process. Below we describe the normal vehicle registration while Figure 3 shows the steps.

1) A user selects its identity id_i and password pw_i and calculates $h(pw_i)$. $(id_i, h(pw_i))$ are sent to the AS using a secure channel.

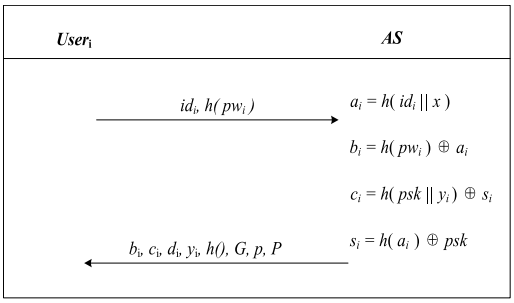


FIGURE 3. Normal vehicle registration phase.

2) Upon receiving parameters $(id_i, h(pw_i))$ from OBU_i, the AS chooses a random number y_i and performs following operations: $a_i = h(id_i||x)$, $b_i = a_i \oplus h(pw_i)$, $c_i = h(psk||y_i) \oplus s_i$, $s_i = h(a_i) \oplus psk$, where s_i is only known by the AS at present and x is the secret key to AS.
3) The AS stores a set of parameters (i.e., b_i, c_i, y_i, $h()$, G, P, P) in the reliable security hardware OBU using a secure channel, where G, P, p are defined in initialization phase.
4) $User_i$ inputs its real identity id_i and password pw_i to OBU_i and selects a number x_i at random as its private key and calculates $P_{pub_i} = x_i P$ as its public key and $z_i = x_i \oplus h(pw_i)$. OBU_i extracts $a_i = b_i \oplus h(pw_i)$ using b_i and pw_i, and then calculates the validate parameter $d_i = h(id_i||pw_i||a_i)$ and stores (P_{pub_i}, z_i, d_i) in its OBU. The parameter z_i protects the security of the private key x_i and can prevent the side channel attack.

C. LOGIN

Vehicle users need to be verified first when they intend to get to access to service from VANETs. The details of the login phase are as followed.

1) $User_i \rightarrow OBU_i$: $User_i$ inputs its real identity id_i and password pw_i to OBU_i.
2) Upon receiving id_i and pw_i, OBU_i recalculates a_i using b_i, then checks whether $h(id_i||pw_i||a_i)$ is equals to d_i or not. If its correct, OBU_i believes the user is legal. If not, the login request will be rejected.

D. PASSWORD CHANGE

This procedure in our scheme is as same as in Zhou et al.'s scheme.

E. GENERAL AUTHENTICATION

When the vehicle intends to establish authentication session, the general authentication will be performed between OBU_i and LE_j. The steps are discussed in this part and showed in Figure 4.

1) OBU_i generates a random number $r_i \in Z_p^*$ and calculates: $aid_i = h(r_i||t_o) \oplus id_i$, $m_1 = h(a_i) \oplus r_i$, $m_2 = h(r_i||aid_i||c_i||y_i||t_o)$, where t_o is the current time stamp of OBU_i and a_i has acquired in the login phase.

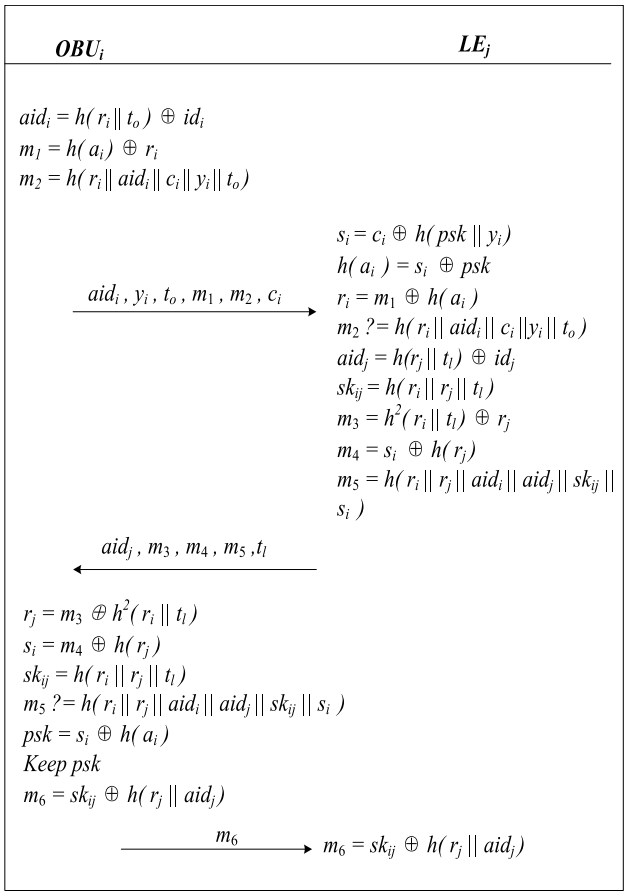


FIGURE 4. Normal vehicle authentication phase.

2) $OBU_i \rightarrow LE_j$: The authentication message (i.e., aid_i, c_i, y_i, m_1, m_2, t_o) is transmitted to LE_j by OBU_i.
3) Upon receiving (i.e., aid_i, c_i, y_i, m_1, m_2, t_o) from OBU_i, LE_j checks t_o is fresh or not firstly. If not, LE_j thinks that there may be a reply attack from an invalid OBU_i. If yes, LE_j calculates s_i using $c_i \oplus h(psk||y_i)$, $h(a_i) = s_i \oplus psk$ and then retrieves $r_i = m_1 \oplus h(a_i)$, and next checks whether $m_2 = h(r_i||c_i||aid_i||y_i||t_o)$ holds or not. If it does, LE_j calculates $aid_j = h(r_j||t_l) \oplus id_j$, where $r_j \in Z_p^*$ is generated randomly by LE_j, the session key $sk_{ij} = h(r_i||r_j||t_l)$, where t_l denotes the current time of LE_j. And then calculates: $m_3 = r_j \oplus h^2(r_i||t_l)$, $m_4 = s_i \oplus h(r_j)$, the verification message $m_5 = h(r_i||r_j||aid_i||aid_j||sk_{ij}||s_i)$. If it does not, the authentication request will be rejected.
4) $LE_j \rightarrow OBU_i$: LE_j transmits the authentication response message (i.e., aid_j, m_3, m_4, m_5, t_l) to OBU_i.
5) On receiving the response message from LE_j, OBU_i firstly checks t_l is fresh or not. If not, OBU_i thinks there may be a reply attack. If yes, OBU_i calculates: $r_j = m_3 \oplus h^2(r_i||t_l)$, $s_i = m_4 \oplus h(r_j)$, $sk_{ij} = h(r_i||r_j||t_l)$. Then, OBU_i checks whether the equation $m_5 = h(r_i||r_j||aid_i||aid_j||sk_{ij}||s_i)$ holds or not. If it does, OBU_i affirms that the LE_j is trustful. Next, OBU_i calculates $m_6 = sk_{ij} \oplus h(r_j||aid_j)$, $c_i^* = h(psk||r_i) \oplus a_i$; and replaces the c_i and y_i with c_i^* and r_i. Actually, OBU_i is trustful now, since it can extract psk using $s_i \oplus h(a_i)$; calculates $e_i = h(pw_i) \oplus psk$ and stores it in its reliable security hardware. In this way, an adversary cannot obtain information to initiate a side channel attack. Otherwise, authentication process will be terminated by OBU_i.
6) OBU_i submits m_6 to LE_j.
7) Upon receiving the message m_6, LE_j calculates:

$$h^*(r_j||aid_j) = sk_{ij} \oplus m_6,$$

then checks $h^*(r_j||aid_j)$ is equal to $h(r_j||aid_j)$ or not. This also can avoid a reply attack from an invalid OBU_i.

F. TRUSTED-EXTENDED AUTHENTICATION

This procedure in our scheme is as same as in Zhou et al.'s scheme.

G. SECURE COMMUNICATION

Two trusted Vehicles can complete this process in the secure communication phase, the following steps are described in this part, as shown in Figure 5.

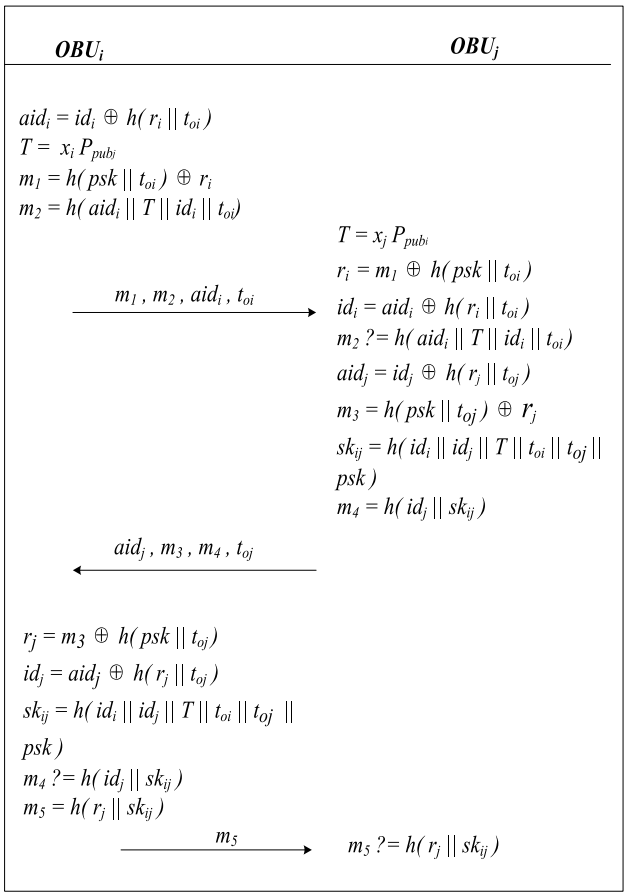


FIGURE 5. Secure communication phase.

1) OBU_i selects a random number r_i and calculates: $aid_i = id_i \oplus h(r_i||t_{oi})$, $T = x_i P_{pub_j}$, $m_1 = h(psk||t_{oi}) \oplus r_i$, and the verification message$m_2 = h(aid_i|| T|| id_i|| t_{oi})$, where $psk = e_i \oplus h(pw_i)$ is obtained from the login phase and t_{oi} denotes the current time stamp of OBU_i.
2) $OBU_i \rightarrow OBU_j$: The request message (i.e., m_1, m_2, aid_i, t_{oi}) is transmitted to OBU_j by OBU_i.
3) On receiving the request message (i.e., m_1, m_2, aid_i, t_{oi}) from OBU_i, OBU_j firstly checks whether t_{oi} is fresh or not. If not, OBU_j thinks there may be a replay attack. If yes, OBU_j calculates T using its own private key and public key of OBU_i, $T = x_j P_{pub_i}$, $r_i = m_1 \oplus psk||t_{oi})$, $id_i = aid_i \oplus h(r_i||t_{oi})$, then checks whether $m_2 = h(aid_i||T||id_i||t_{oi})$ is equal to m_2 or not. If it's, OBU_j selects a random number r_j and calculates: $aid_j = id_j \oplus h(r_j||t_{oj})$, $m_3 = h(psk||t_{oj}) \oplus r_j$, $sk_{ij} = h(id_i||id_j||T||t_{oi}||t_{oj}||psk)$, $m_4 = h(id_j||sk_{ij})$.
4) $OBU_j \rightarrow OBU_i$: OBU_j submits its response message (i.e., m_3, m_4, aid_j, t_{oj}) to OBU_i.
5) Upon receiving the response message (i.e., m_3, m_4, aid_j, t_{oj}) from OBU_j, where t_{oj} denotes the current time stamp of OBU_j, OBU_i firstly checks whether t_{oj} is fresh or not. If not, OBU_i thinks there may be a reply attack. If yes, OBU_i calculates: $r_j = m_3 \oplus h(psk||t_{oj})$, $id_j = aid_j \oplus h(r_j||t_{oj})$, $sk_{ij} = h(id_i||id_j||T||t_{oi}||t_{oj}||psk)$ and then checks whether $h(id_j||sk_{ij})$ is equal to m_4 or not. If its, OBU_i calculates the reply message $m_5 = h(r_j||sk_{ij})$. If not, the process will fail.
6) OBU_i submits its reply message m_5 to OBU_j.
7) Upon receiving the message m_5, OBU_j recalculates $h(r_j||sk_{ij})$ and checks whether $m_5 = h(r_j||sk_{ij})$ holds or not. If yes, the OBU_i and OBU_j both reach the trust threshold of each other. So, they can communicate securely using the sk_{ij} session key to ensure communication security. If not, the process will be terminated.

H. KEY REVOCATION

This procedure in our scheme is the same as the Zhou et al.'s scheme which is same as the TEAM.

I. KEY UPDATE

The key update procedure will be triggered when the TV's key lifecycle is coming to an end. The process is displayed as follows.

1) OBU_i selects a number r_i randomly to calculate $m_1 = r_i \oplus psk_{old}$, $m_2 = msg_{kup} \oplus psk_{old}$, $m_3 = h(r_i||t_{oi}||msg_{kup})$, where t_{oi} is the current time stamp of OBU_i.
2) OBU_i submits the key update request (i.e., m_1, m_2, m_3, t_{oi}) to LE_j.
3) Upon receiving (i.e., m_1, m_2, m_3, t_{oi}) from OBU_i, LE_j firstly checks t_{oi} is fresh or not. If not, LE_j considers there may be a reply attack. If yes, then LE_j recalculates $r_i = m_1 \oplus psk_{old}$, $msg_{kup} = m_2 \oplus psk_{old}$; checks whether $h(r_i||t_{oi}||msg_{kup})$ is equal to m_3. If it's, LE_j believes OBU_i is trustful. Then, LE_j chooses a random number r_j to calculate $m_4 = r_j \oplus h(r_i||t_{lj})$, $m_5 = psk_{new} \oplus h(r_j||t_{lj})$, $m_6 = h(r_i||r_j||psk_{new}||t_{lj})$, where t_{lj} is the current time stamp of LE_j. Next, LE_j calculates $sk_{ij} = h(r_i||r_j||psk_{new}||t_{oi}||t_{oj})$.
4) The reply message (m_4, m_5, m_6, t_{lj}) is sent by LE_j to OBU_i.
5) Upon receiving (m_4, m_5, m_6, t_{lj}), OBU_i firstly checks t_{lj} is fresh or not. If not, OBU_i considers there may be a reply attack. If yes, OBU_i retrieves $r_j = m_4 \oplus h(r_i||t_{lj})$, $psk_{new} = m_5 \oplus h(r_j||t_{lj})$; checks whether $h(r_i||r_j||psk_{new}||t_{lj})$ is equal to m_6. If it's, OBU_i believes LE_j is trustful.
6) OBU_i updates the authentication parameter psk using psk_{new}, and recalculates the session key $sk_{ij} = h(r_i||r_j||psk_{new}||t_{oi}||t_{oj})$ to be used for the secure communication between two trusted vehicles.

VII. SECURITY ANALYSIS

To illustrate security, the security analysis of our proposed scheme in this section will be analyzed. First, the formal security analysis is given to prove our proposed scheme is secure. Second, we apply the informal security analysis to show the feasibility of coming up with security requirements in VANETs.

A. SECURITY MODEL

The capabilities of the adversary and security requirements of the mutual authentication protocol are presented in this subsection. The security model of our proposed improved scheme is realized by the game between an adversary A and a challenger. Our security proofs adopt a random oracle model from Bellare et al. [28]. Concrete security requirements can be referred to [26]. An adversary A can be a probabilistic polynomial time machine [28]. When A gets access to all the possible oracles, which are described as below, we allow it to potentially control both the general authentication process and the secure communication process in our improved scheme. Both OBU V_i and LE L_i are a participant. Let U_i^i denote the ith instance U_i, where U denotes all participants, and they all could be considered to be an oracle.

Definition 1 (Adversary Abilities):

- Execute(V_i^i, U_i^i): This query tests the adversary's passive attack ability. The adversary A is allowed to get access to the honest general authentication procedure and the communication procedure. This query is answered with the honest execution transcripts of the proposed protocol.
- Send(U_i^i, m_0): This query tests the adversary's active attack ability. A could transmit a message m_0 to the oracle U_i^i. On receiving this request message m_0, the result and answer are returned to A by the oracle according to the proposed protocol.
- Reveal(U_i^i): In this query, the oracle simulates a known key attack. The adversary A could get a session key from

the oracleU_i^j, if the oracle has obtained a session key. Otherwise, it returns $\perp$ to the adversary.

- Corrupt(V_i^j): In this query, the oracle simulates a violent attack. It allows the adversary A to get access to U_i^j's secret information stored in the vehicle's OBU.
- Test(U_i^j): This query tests the AKE security of the U_i^j's session key. The adversary A could ask the oracle for the real session key at most once. On receiving this test query, the oracle outputs an unbiased bit value b. If b is equal to 1, the oracle will return the session key to A. Otherwise, it returns $\perp$ to A.

Definition 2 (Freshness): An instance U_i^j is fresh unless one of following situations occurs:

1) The Reveal-query has been sent by U_i^j or its partner.
2) The adversary A queries the Corrupt(V_i^j) at the meantime.
3) Before U_i^j or its partner sent the Test-query, they had already been sent the Corrupt-query.

Definition 3 (Semantic Security): Let the adversary As ability to beat our protocol be the probability of guessing the bit b got involved in the Test session. To be specific, let's define the advantage of A to be: our scheme is AKE-secure if $Adv^{ake}_{O2L/O2O}(A)$ is negligibly greater than $max\{(q_s/|D|, \varepsilon)\}$ with q_s Send-queries at the most, where $|D|$ is the space of the password dictionary.

B. THE FORMAL SECURITY ANALYSIS

The formal security analysis under the random oracle model is given from aspects of its theorems as well as its corresponding proofs in detail. The details are displayed as follows.

Theorem 1: We define G_p be the elliptic curve group, $O2L$ be an event that the adversary A could control the general authentication procedure between OBU and LE. Let D be a password dictionary following a uniformly distributed and its size is $|D|$. Let 2^l be the space of the Hash Function, where l denotes the bit length of Hash values. And let A denote an adversary against the general authentication procedure of our scheme by executing at the most q_e Execute-queries, q_s Send-queries and q_h Hash-queries. Then we have:

$$Adv^{ake}_{O2L}(A) = \frac{q_h^2}{2^l} + 2q_s max\left\{\frac{1}{|D|}, \varepsilon)\right\}.$$

Proof of Theorem 1: We demonstrate that the proposed protocol is provably secure with Exp_0, Exp_1, Exp_2, Exp_3, Exp_4. Let Su_n $(1 \le n \le 4)$ denote the event that A successfully guesses b from the Test-query.

Experiment Exp_0: This experiment models a real attack. According to our definition $Adv^{ake}_{O2L}(A)$, we have:

$$F_0 = Adv^{ake}_{O2L}(A) = 2Pr[Su_0] - 1.$$

Experiment Exp_1: All oracles Execute, Send, Reveal, Corrupt, Test in this experiment are modeled. The adversary A cannot distinguish Exp_0 and Exp_1. Hence,

$$F_1 = |Pr[Su_0] - Pr[Su_1]| = 0.$$

Experiment Exp_2: In this experiment, all oracles are also simulated. There is a collision in Exp_2. If the collision occurs, the adversary A will initiate a reply attack to win the game. We can have the probability of collisions according to the birthday paradox. Hence,

- If there's a hash collision occurs, the probability of the collision at most is $\frac{q_h^2}{2^{l+1}}$.

So, only in above case can Exp_1 and Exp_2 be distinguished, and:

$$F_2 = |Pr[Su_2] - Pr[Su_1]| \le \frac{q_h^2}{2^{l+1}}.$$

Experiment Exp_3: Now, all oracles have been modeled in Exp_3. Once the adversary A obtains the correct session key: $sk = h(r_i||r_j||t_l)$, the invalid OBU_i could extract the pre-shared key between LE and AS. However, A could do nothing with only b_i, c_i, d_i, y_i, z_i and P_{pub_i}, because r_i, r_j is required for A to break a session key. Hence, we have a hypothesis that A has queried Corrupt(V_i^j). If A intends to break the session key $sk = h(r_i||r_j||t_l)$, it must compute r_i, r_j with the value a_i, where $a_i = b_i \oplus h(pw_i)$. However, it is hard to recover a_i without the correct password pw_i. A asks Corrupt(V_i^j) and guesses pw_i from the dictionary D with maximum q_s Send-queries. Therefore, the probability at most is $\frac{q_s}{|D|}$. Then we have:

$$F_3 = |Pr[Su_3] - Pr[Su_2]| \le q_s max\left\{\frac{1}{|D|}, \varepsilon)\right\}.$$

Experiment Exp_4: Besides, we say that A succeeds the $O2L$ of the scheme if A uses the Test(U_i^j) oracle and returns the real bit guess. Thus,

$$F_4 = Pr[Su_3] = \frac{1}{2}.$$

Therefore, from F_1, F_2, F_3, F_4, we have:

$$\begin{aligned} |Pr[Su_0] - \frac{1}{2}| &= |Pr[Su_0] - Pr[Su_3]| \\ &\le |Pr[Su_0] - Pr[Su_1]| \\ &\quad + |Pr[Su_1] - Pr[Su_2]| \\ &\quad + |Pr[Su_2] - Pr[Su_3]| \\ &= F_1 + F_2 + F_3 \\ &\le \frac{q_h^2}{2^{l+1}} + q_s max\left\{\frac{1}{|D|}, \varepsilon)\right\}. \end{aligned}$$

Hence, from F_0 we will have:

$$Adv^{ake}_{O2L}(A) \le \frac{q_h^2}{2^l} + 2q_s max\left\{\frac{1}{|D|}, \varepsilon)\right\}.$$

Theorem 2: Let $O2O$ be an event that A could violate the secure communication procedure between OBU_i and OBU_j of two trusted vehicles. D_{id} and D are identity dictionary with the size of $|D_{id}|$ and identity dictionary with the size of $|D|$ respectively and both of them follow a uniformly distributed. Let Adv_A^{ECDHP} be the advantage for A in solving the ECCDHP in a polynomial time. Let A denote an adversary against the

secure communication procedure. Let $|Hash|$ denote the Hash function space. And within the time complexity limit t, A can only issue at the most q_e Execute-queries, q_s Send-queries, q_h Hash-queries. Hence,

$$\begin{aligned} Adv^{ake}_{O2O}(A) \leq & \frac{2(q_s+q_e)}{|D_{id}|} + \frac{q_h^2+2q_s}{2^l} + \frac{(q_s+q_e)^2}{p} \\ & + 2q_s max\left\{\frac{1}{|D|}, \varepsilon)\right\} \\ & + 2q_h((q_s+q_e)^2+1) \\ & * Adv^{ake}_{O2O}(A)(t+(q_e+q_s)t_m). \end{aligned}$$

Proof of Theorem 2:

Experiment Exp_0: This experiment models a real attack. According to our definition $Adv^{ake}_{O2O}(A)$, we have

$$Adv^{ake}_{O2O}(A) = 2Pr[Su_0] - 1.$$

Experiment Exp_1: All oracles Execute, Send, Reveal, Corrupt, Test in this experiment are modeled. The adversary A cannot distinguish Exp_0 and Exp_1. Hence,

$$F_1 = |Pr[Su_1] - Pr[Su_0]| = 0.$$

Experiment Exp_2: Here, all the oracles Send, Execute, Reveal, Corrupt, and Test are also modeled in this experiment. Once A gets the real identity id_i of trusted OBU_i, id_j of trusted OBU_j from the identity space, we stop simulating this guessing identity attacks.

So, Exp_2 and Exp_1 cannot be distinguished unless the case appears, and:

$$F_2 = |Pr[Su_2] - Pr[Su_1]| \leq \frac{q_s+q_e}{|D_{id}|}.$$

Experiment Exp_3: In this experiment, all oracles are also simulated. There exist two styles of collisions in Exp_3. If both collisions occur, the adversary A will initiate a reply attack to win the game. We can have the probability of collisions according to the birthday paradox. Hence,

- If there's a hash collision occurs, the probability of the collision at most is $\frac{q_h^2}{2^{l+1}}$.
- If there's a collision between the random number r_i and r_j, the probability of the collision at most $\frac{(q_s+q_e)^2}{2p}$.

So, only in following cases can Exp_1 and Exp_2 be distinguished, and:

$$F_3 = |Pr[Su_3] - Pr[Su_2]| \leq \frac{q_h^2}{2^{l+1}} + \frac{(q_s+q_e)^2}{2p}.$$

Experiment Exp_4: Here, all the oracles that have been modeled in Exp_3 are also modeled in this experiment. When Corrupt(V_i^i) is queried, the adversary A can extract the information b_i, c_i, d_i, y_i, z_i, P_{pub_i} and e_i stored in the vehicle's OBU, To break the session key, A needs to know the secret key x_i, psk, id_i, id_j and the random number r_i as well as r_j. It is difficult to recover psk and x_i from the information b_i, c_i, d_i, y_i, z_i, P_{pub_i} and e_i without getting the correct password. The adversary cannot get the user password, since there is no user password in the whole communication message. So, we have:

$$F_4 = |Pr[Su_4] - Pr[Su_3]| \leq q_s max\left\{\frac{1}{|D|}, \varepsilon)\right\}.$$

Experiment Exp_5: Here and now, all oracles in Exp_4 have been modeled. In this experiment, we consider the probability that A forges the authentication value m_2, m_4, m_5 without using random oracles for corresponding queries. Unless the oracle can stop the game with right values, Exp_5 becomes indistinguishable from Exp_4 to A. Hence, we will have:

$$F_5 = |Pr[Su_5] - Pr[Su_4]| \leq \frac{q_s}{2^l}.$$

Experiment Exp_6: Here and now, Exp_6 will simulate the hash oracle h to break the session key $sk = h(id_i||id_j||x_iP_{pub_j}||psk||t_{oi}||t_{oj})$. Computing $x_iP_{pub_j}$ belongs to ECCDHP. The case when the adversary A queries the oracle h on $id_i||id_j||x_iP_{pub_j}||psk||t_{oi}||t_{oj}$, and the oracle responds the value as follows: $id_i||id_j||x_iP_{pub_j}||psk||t_{oi}||t_{oj}||ECCDH(x_jP_{pub_i}, P_{pub_i}) + ECCDH(x_iP_{pub_j}, P_{pub_j})$. So, Exp_5 and Exp_4 cannot be distinguished unless the above case occurs. We define the advantage of A as $Adv^{ake}_{O2O}(A)$ $(t+(q_e+q_s)tm)$, while t is the maximum time and t_m is the point multiplication time based on ECC. A can win the game at the fewest q_h hash-queries. Then, we have:

$$\begin{aligned} F_6 &= |Pr[Su_6] - Pr[Su_5]| \\ &\leq q_h Adv^{ake}_{O2O}(A)(t+(q_e+q_s)t_m). \end{aligned}$$

Experiment Exp_7: In this experiment, we suppose that A has issued Corrupt(V_i^i) after the previous Test query. Similar to the Exp_6, if the session key sk can be obtained in the hash oracle h, the probability that x_i and x_j are in the same session is $\frac{1}{(q_s+q_e)^2}$. So we will have:

$$\begin{aligned} F_7 &= |Pr[Su_6] - Pr[Su_5]| \\ &\leq q_h(q_s+q_e)^2 Adv^{ake}_{O2O}(A)(t+(q_e+q_s)t_m). \end{aligned}$$

Besides, A will succeed against an oracle, if the Test query return it the real bit Guess randomly. So, we have:

$$F_8 = Pr[Su_7] = \frac{1}{2}.$$

Therefore, from F_1, F_2, F_3, F_4, F_5, F_6 and F_7 we have:

$$\begin{aligned} |Pr[Su_0] - \frac{1}{2}| &= |Pr[Su_0] - Pr[Su_7]| \\ &\leq |Pr[Su_0] - Pr[Su_1]| \\ &\quad + |Pr[Su_1] - Pr[Su_2]| \\ &\quad + |Pr[Su_2] - Pr[Su_3]| \\ &\quad + |Pr[Su_3] - Pr[Su_4]| \\ &\quad + |Pr[Su_4] - Pr[Su_5]| \\ &\quad + |Pr[Su_5] - Pr[Su_6]| \\ &\quad + |Pr[Su_6] - Pr[Su_7]| \\ &= F_1 + F_2 + F_3 + F_4 + F_5 + F_6 + F_7 \\ &\leq \frac{q_s+q_e}{|D_{id}|} + \frac{q_h^2}{2^{l+1}} + \frac{(q_s+q_e)^2}{2p} + \frac{q_s}{2^l} \end{aligned}$$

$$+ q_s max\left\{\frac{1}{|D|}, \varepsilon)\right\}$$
$$+ q_h((q_s + q_e)^2 + 1)$$
$$* Adv^{ake}_{O2O}(A)(t + (q_e + q_s)t_m).$$

Hence, from F_0 we will have:

$$Adv^{ake}_{O2O}(A) \leq \frac{2(q_s + q_e)}{|D_{id}|} + \frac{q_h^2 + 2q_s}{2^l} + \frac{(q_s + q_e)^2}{p}$$
$$+ 2q_s max\left\{\frac{1}{|D|}, \varepsilon)\right\}$$
$$+ 2q_h((q_s + q_e)^2 + 1)$$
$$* Adv^{ake}_{O2O}(A)(t + (q_e + q_s)t_m).$$

C. OTHER DISCUSSIONS

1) Resistance to insider attack enhancement: If the real password is stored in plaintext form in AS, the AS may careless use of it. So in our scheme $User_i$ sends its $(id_i, h(pw_i))$ to AS. AS cannot recalculate the password because of the one-way feature of the hash function. So AS cannot misuse the password.
2) Anonymity, Identity Privacy-Preserving and the location privacy of user Enhancement: If the anonymity has not changed for a long time, the adversary can still steal the trajectory privacy. If the real user's identity is transmitted in plaintext form on VANETs, it can be analyzed the message easily by the attack. In our scheme, we also use XOR operation with a hash to increase the security of anonymous identity. However, the hash takes a timestamp to connect to a random as an input. We use double security parameters (random number, timestamp) to change anonymity dynamically. Above all, the adversary cannot get the user privacy by intercepting information.
3) Secure session key enhancement: Although in Zhou et al.'s scheme, the session key is diverse in different authentication or communication phase, the session key can be leaked by guessing the identity from the identity space, the explanation is described in the following 5) in detail. In our scheme, the session key is secure and also change dynamically because of the hash of the current time. The reasons of security are also demonstrated in the following 5).
4) Resistance to password guessing attack: Since there is no user password in the whole communication message, the adversary cannot obtain the user password.
5) Resistance to identity guessing and impersonation attack: Assuming D_{id} denotes the size of the identity space, a adversary guesses a id_i^* from a uniformly distributed identity dictionary D_{id} of OBU_i and computes the following parameters in Zhou et al.'s scheme:

$$h^*(r_i) = aid_i \oplus id_i^*,$$
$$r_j^* = m_3 \oplus [h^*(r_i)]^2,$$
$$psk^* = r_j^* \oplus m_4,$$
$$a_i^* = h(psk^*||y_i) \oplus c_i,$$
$$r_i^* = m_1 \oplus h(a_i^*),$$
$$sk_{ij} = h(r_i^*||r_j^*).$$

And then compares the $h(r_i^*)? = h^*(r_i)$, if yes, the adversary guess the id_i of OBU_i successfully. Next, the $sk_{ij} = h(r_i^*||r_j^*)$ also be guesses successfully by the adversary. Therefore, Zhou et al.'s scheme still has security threats. In our scheme, assuming that the adversary also guesses a id_i^* from the $\mathcal{L}$ of OBU_i and computers sk_{ij} that is generated by the hash that takes random number r_i, r_j as the input. r_i, r_j are encrypted by key a_i, and a_i is known by AS and trustful OBU. Therefore, our scheme can resist to identity guessing attack, but Zhou et al.'s cannot.
6) Resistance to reply attack: In our proposal, all the transmitted messages contain current time stamps, so these messages must pass the check of the time stamp freshness firstly. Therefore, a reply attack from an adversary is prevented.

VIII. PERFORMANCE ANALYSIS

A. COMPUTATION COST

To demonstrate the efficiency of our proposed scheme, we analyze computation cost of the authentication and secure communication phase respectively. The following display is the performance analysis of [23] and our scheme. We analyze the computation and communication cost by contrast between our proposed scheme and [23]. These symbols T_h, T_m, T_a respectively illustrate the execution time of shs-hash-256, scalar point multiplication and scalar addition multiplication based on ECC. These related operations are based upon the miracl c++ library [29]. In our scheme, the machine parameters are Intel(R) Core(TM) i5-3337U CPU, 1.8GHz and RAM is 4GB on a Windows 10 PC.

As shown in TABLE 2, 3, 4, the authentication time of [23] is about 17 $T_h \approx 0.170$ ms, the authentication time of our scheme is about $18T_h \approx 0.180$ ms, the communication time of [23] is about $12T_h + 10T_m + 6T_a \approx 12T_h + 10T_m \approx 29.900$ ms, and $T_a \ll T_m, T_h$. Then the communication time of our scheme is about $16T_h + 2T_m \approx 6.116$ ms. As shown in Figure 6, TABLE 5, [23] is slightly lighter

TABLE 2. The execution time of basic operation.

Operations	Time(ms)
T_h	0.010
T_m	2.978

TABLE 3. The Authentication cost and total execution time of each scheme.

Operations	Authentication Cost	Total Time(ms)
[23]	$17\,T_h$	≈0.170
Our Proposed	$18\,T_h$	≈0.180

TABLE 4. The communication cost and total execution time of each scheme.

Operations	Communication Cost	Total Time(ms)
[23]	$12T_h$+$10T_m$+$6T_a$	≈29.900
Our Proposed	$16T_h$+$2T_m$	≈6.116

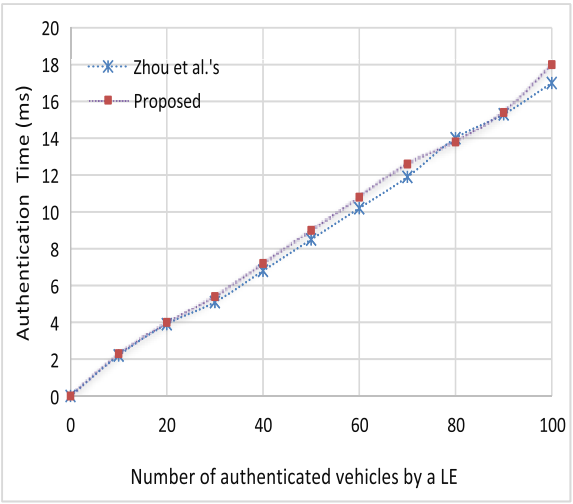


FIGURE 6. Comparison of authentication cost.

TABLE 5. Comparison of security features

	[23]	Ours
Resistance To Insider Attack		✓
Resistance To Session Key Disclosure		✓
Resistance To User Traceability Attack		✓
Resistance To Reply Attack	✓	✓
Resistance To Identity Guessing Attack		✓
Provides User Anonymity	✓	✓
Low Consumption		✓

than our scheme in authentication cost, however, it cannot meet security requirements that we know about. As shown in Figure 7, it is noteworthy that the communication cost of our scheme is far more lightweight than [23], so our scheme yields better efficiency than previously proposed scheme in VANETs. At the same time, our scheme can resist malicious attacks which have been analyzed in section VII and shown in TABLE 5. Therefore, our scheme is a robust improvement of the privacy-preserving authentication scheme.

B. RSU SERVING CAPABILITY

When getting into the DSRC communication coverage of a LE/trusted vehicle in the area of RSU, the mistrusted vehicle will firstly build a mutual authentication with the LE/trusted vehicle. After the authentication process is finished, trusted vehicles can communicate with each other. RSU can broadcast some safety information SI, such as school zone, traffic signal, or accident zone periodically to trusted vehicles.

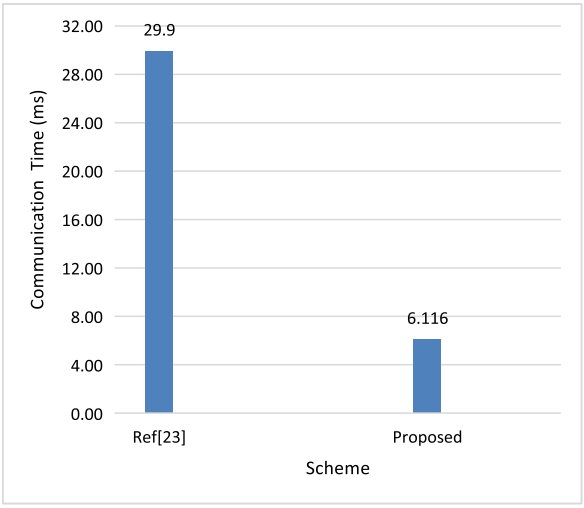


FIGURE 7. Consumption time of each scheme.

We calculate RSU serving capability on the basis of the formula defined in [30] $RSU_{ser} = \frac{p \cdot T_{com} \cdot r}{s \cdot d}$, where p, r, T_{com}, s, and d respectively denote the probability for RSU to send SI messages to the trusted vehicles within its communication range r (200m), the communication time between RSU and trusted vehicles, the average speed of a trusted vehicle, the number of trusted vehicles. In our scheme, we assume that the T_{com} is as same as between two trusted vehicles', $16T_h + 2T_m \approx 6.116$ ms.

As shown in Figure 8, we can see that $8 \leq s \leq 10$, $200 \leq d \leq 400$. It can be observed that the performance of the RSU in our scheme is effective. RSU can generate 33 session keys and communicate with corresponding trusted vehicles for each 200 ms. We also have an observation that RSU_{ser} is directly proportional to r and inversely proportional to the

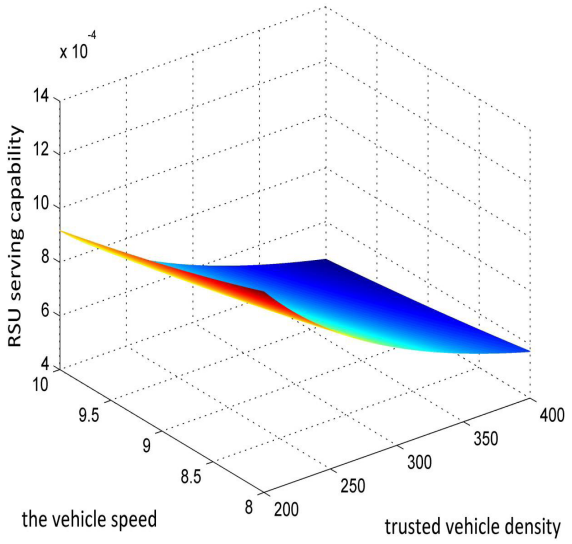


FIGURE 8. RSU serving capacity under different speed and the number of vehicles.

number d and the speed s of trusted vehicles. We can calculate that a LE can authenticate about 200 mistrusted vehicles for each 200 ms due to the limit of the vehicle density, but 1111 in theory. Hence, we come to the conclusion that our scheme has lower message loss than Zhou et al.'s when the vehicle density inside the communication area enlarges.

IX. CONCLUSIONS

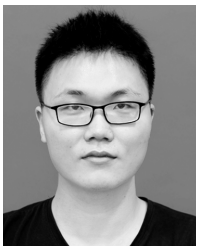
We find that Zhou et al.'s scheme cannot achieve some of vital security requirements due to its vulnerability to identity guessing attack and impersonation attack in this paper. In addition, to overcome the weakness of Zhou et al.'s scheme, by using elliptic curves encryption technology, a new efficient privacy-preserving mutual authentication scheme for secure V2V communication has been proposed by us. The security analysis suggests that this scheme can eliminate the security vulnerability of the previously proposed authentication scheme. The performance evaluation and analysis of the calculating result indicate that our proposed authentication scheme yields reasonable cost since it has lower computation and communication overhead than the previous one. Hence, our improvement is more effective and securer in the VANET environment.

REFERENCES

[1] F.-Y. Wang, D. Zeng, and L. Yang, "Smart cars on smart roads: An ieee intelligent transportation systems society update," *IEEE Pervasive Comput.*, vol. 5, no. 4, pp. 68–69, Oct./Dec. 2006.
[2] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.
[3] K. Hwang and M. Chen, *Big-Data Analytics for Cloud, IoT and Cognitive Computing*. Hoboken, NJ, USA: Wiley, 2017.
[4] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2740–2749, Oct. 2017.
[5] S. Kumari, M. Karuppiah, X. Li, F. Wu, A. K. Das, and V. Odelu, "An enhanced and secure trust-extended authentication mechanism for vehicular ad-hoc networks," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4255–4271, 2016.
[6] M. Chen, Y. Hao, K. Lin, L. Hu, and Z. Yuan, "Label-less learning for traffic control in an edge network," *IEEE Netw.*, vol. 32, no. 6, pp. 8–14, Nov. 2018.
[7] B. Liu, D. Jia, J. Wang, K. Lu, and L. Wu, "Cloud-assisted safety message dissemination in VANET–cellular heterogeneous wireless network," *IEEE Syst. J.*, vol. 11, no. 1, pp. 128–139, Mar. 2017.
[8] B. Liu *et al.*, "Infrastructure-assisted message dissemination for supporting heterogeneous driving patterns," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2865–2876, Oct. 2017.
[9] L. Wu, J. Wang, K. R. Choo, and D. He, "Secure key agreement and key protection for mobile device user authentication," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 319–330, Feb. 2019.
[10] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, "A privacy preserving three-factor authentication protocol for e-health clouds," *J. Supercomput.*, vol. 72, no. 10, pp. 3826–3849, 2016.
[11] Q. Jiang, J. Ma, X. Lu, and Y. Tian, "An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks," *Peer-Peer Netw. Appl.*, vol. 8, no. 6, pp. 1070–1081, Jun. 2014.
[12] Q. Jiang, J. Ma, G. Li, and X. Li, "Improvement of robust smart-card-based password authentication scheme," *Int. J. Commun. Syst.*, vol. 28, no. 2, pp. 383–393, 2015.
[13] Y. Xie, L. Wu, N. Kumar, and J. Shen, "Analysis and improvement of a privacy-aware handover authentication scheme for wireless network," *Wireless Pers. Commun.*, vol. 93, no. 2, pp. 523–541, 2017.
[14] L. Wu, Y. Xia, Z. Wang, and H. Wang, "Be stable and fair: Robust data scheduling for vehicular networks," *IEEE Access*, vol. 6, pp. 32839–32849, 2018.
[15] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 8–15, Oct. 2006.
[16] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed iot applications," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2014, pp. 2728–2733.
[17] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE 27th Conf. Comput. Commun. (INFOCOM)*, Apr. 2008, pp. 1229–1237.
[18] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-zones for location privacy in vehicular networks," in *Proc. ACM Workshop Wireless Netw. Intell. Transp. Syst. (WiN-ITS)*, 2007, pp. 1–7.
[19] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proc. IEEE Int. Conf. Commun.*, May 2008, pp. 1451–1457.
[20] J. Zhang and Y. Xu, "Privacy-preserving authentication protocols with efficient verification in VANETs," *Int. J. Commun. Syst.*, vol. 27, no. 12, pp. 3676–3692, 2014.
[21] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," in *Proc. 6th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Netw. (SECON)*, Jun. 2009, pp. 1–9.
[22] L.-Y. Yeh, Y.-C. Chen, and J.-L. Huang, "PAACP: A portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks," *Comput. Commun.*, vol. 34, no. 3, pp. 447–456, 2011.
[23] Y. Zhou, X. Zhao, Y. Jiang, F. Shang, S. Deng, and X. Wang, "An enhanced privacy-preserving authentication scheme for vehicle sensor networks," *Sensors*, vol. 17, no. 12, p. 2854, 2017.
[24] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. 27th Conf. Comput. Commun. (INFOCOM)*, Apr. 2008, pp. 246–250.
[25] C. Zhang, P.-H. Ho, and J. Tapolcai, "On batch verification with group testing for vehicular communications," *Wireless Netw.*, vol. 17, no. 8, pp. 1851–1865, 2011.
[26] M. C. Chuang and J. F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," *IEEE Syst. J.*, vol. 8, no. 3, pp. 749–758, Sep. 2014.
[27] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2012, pp. 538–552.
[28] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2000, pp. 139–155.
[29] *Rational Arithmetic C++ Library*, MIRACL, London, U.K., 2013.
[30] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017.
[31] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Gener. Comput. Syst.*, vol. 84, pp. 216–227, Jul. 2018.
[32] P. Vijayakumar, V. Chang, L. J. Deborah, B. Balusamy, and P. G. Shynu, "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," *Future Generat. Comput. Syst.*, vol. 78, pp. 943–955, Jan. 2016.

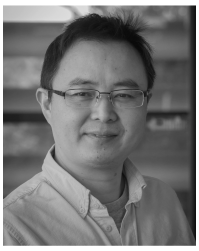
LIBING WU received the B.S. and M.S. degrees in computer science from Central China Normal University, Wuhan, China, in 1994 and 2001, respectively, and the Ph.D. degree in computer science from Wuhan University, China, in 2006, where he is currently a Professor with the School of Computer Science. His areas of research interests include distributed computing, trusted software, and wireless sensor networks. He is a Senior Member of the CCF.

QIANQIAN SUN is currently pursuing the master's degree in cyberspace security. Her research interests include wireless networks, vehicular ad-hoc networks, cryptography, and information security.



XINPEI WANG is currently pursuing the master's degree. His research interests include computer software and theory.

JING WANG received the B.S. degrees in computer science from Wuhan University, Wuhan, China, in 2016, where she is currently pursuing the Ph.D. degree with the School of Computer Science. Her main research interests include cryptography and information security; in particular, secure cloud storage and cryptographic protocols.



SHUI YU is currently a Full Professor with the School of Software, University of Technology Sydney, Australia. He has published two monographs and has edited two books, over 200 technical papers, including top journals and top conferences, such as the IEEE TPDS, TC, TIFS, TMC, TKDE, TETC, ToN, and INFOCOM. His research interests include security and privacy, networking, big data, and mathematical modelling.

YIFEI ZOU received the B.E. degree from Computer School, Wuhan University, in 2016. He is currently pursuing the Ph.D. degree with the Department of Computer Science, The University of Hong Kong. His research interests include wireless networks, vehicular ad-hoc networks, and distributed computing.

BINGYI LIU received the B.Sc. degree in computer science from the Wuhan Institute of Technology, Wuhan, China, in 2011. He is currently pursuing the Ph.D. degree under a joint program with the Department of Computer Science, Wuhan University, Wuhan, and the Department of Computer Science, City University of Hong Kong, Hong Kong. His research interests include wireless networks, vehicular ad-hoc networks, and the Internet of Things.

ZIKE ZHU, photograph and biography not available at the time of publication.