IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 22, 2018, accepted November 7, 2018, date of publication November 12, 2018,
date of current version December 18, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2880984

A Robust Authentication Scheme With Continuously Updated Information for Vehicular Sensor Networks

XIN LIU AND RUISHENG ZHANG
School of Information Science and Engineering, Lanzhou University, Lanzhou 730030, China
Corresponding author: Ruisheng Zhang (zhangrs@lzu.edu.cn)

ABSTRACT Traffic accidents frequently occur due to the mistakes of drivers, and many people are injured or lose their lives in this way. However, with the increasing use of Internet of Things in real applications, vehicle sensor networks (VSNs), which able to address this problem, are becoming an important technology for the safety and convenience of humans. Since the associated messages from VSNs are transmitted via public channels, they are vulnerable to attack, as a result of which many network security measures have been widely studied and applied in this context, including the authentication and key agreement scheme. Existing schemes often adopt the third party as the trusted authority to centrally complete the authentication between the vehicles and roadside units. However, a centralized authentication requires cumbersome processes and significantly relies on the security of the trusted authority. In this case of high-speed vehicles, the authentication scheme must be efficient and practical and this requires that the authentication should be more direct and the computational, and communication overhead for authentication should be as low as possible to enable a real-time response. In this paper, we propose a robust authentication scheme with continuously updated information for VSNs through a decentralized authentication for vehicle-to-roadside unit communication. To the best of our knowledge, our approach is the first to adopt the continuously updated information in the authentication process. As the information is temporary and confidential, this innovation guarantees that vehicles may continue driving without the need to stop for key updates, and also enables the transmitted message to be dynamic and confidential. Through a detailed security and performance analysis, our scheme has been demonstrated to be able to resist various types of attacks and offers an improved tradeoff between security and efficiency compared to other schemes.

INDEX TERMS Authentication, continuously updated information, decentralized, security and privacy, fast-authentication.

I. INTRODUCTION

Many people are injured or lose their lives each year due to the frequent occurrence of traffic accidents. According to a report by the World Health Organization, there are 1.25 million traffic-related deaths annually worldwide [1]. Improved safety in traffic scenarios has thus become a top concern, and with the development of wireless technologies, wireless sensor networks (WSNs) are now more widely used for intelligent transportation systems. This new network technology, known as Vehicle Sensor Networks (VSNs), is the most popular approach to providing safer traffic and improved convenience for humans [2]. VSNs are comprised of vehicle-to-roadside unit communications (V2R) and vehicle-to-vehicle communications (V2V) [3]. VSNs also collect real-time traffic-related data, support autonomous vehicle (AV) functions, and provide safety applications for driving, such as the sharing of traffic conditions, intelligent assistance to prevent traffic jams, crash and intersection collision avoidance, and navigation information [4].

The transmitted traffic information is critical as it can affect the decisions taken by other drivers and can lead to traffic accidents if invalid or inaccurate. As the communication channel for V2R and V2V is wireless and publicly accessible, VSNs are vulnerable to adversarial ($\mathcal{A}$) attacks and the security of these networks is very important. The following core security requirements for VSNs have been proposed by Engoulou *et al.* [5] which are: 1) Authentication; the vehicle must authenticate the legality of user (U) and the

message receivers must authenticate the legality of the senders. 2) Integrity and non-repudiation of the message; the receivers must validate the integrity of the transmitted message and the sender must not deny transmission of the message. 3) Anonymity; $\mathcal{A}$ cannot obtain the identity of U or AV through the transmitted message. 4) Unlinkability; $\mathcal{A}$ cannot trace the sender from static information. 5) Low overhead; the computational cost and communication overhead required to satisfy the security requirements should be minimized. 6) Insider attack; if the authenticated U or AV is malicious, it cannot present risk to other AVs.

Among these requirements, authentication is the most vital step to achieving an effective VSN security. This process not only authenticates the legality of both U and the sender, but also negotiates a temporary session key (SK) for the pending V2R and V2V communications. Most proposed schemes adopt the trusted authority (TA) to verify the legality of the AV during the V2R phase, which is referred to as a centralized authentication scheme with a trusted third party. However, any new scheme that might be developed should be safer, require less overhead, and also be decentralized [6]. In order to resist tracing and internal attacks, some schemes adopt a hash chain to render the transmitted message dynamic [7], [8]. However, vehicles must nonetheless stop for key updates due to the short period of the hash chain. In this paper, we design a decentralized scheme that allows only the TA to participate in the registration of U, with the Road Side Unit (RSU) authenticating the Onboard Unit (OBU) directly during the V2R phase. This decentralized design reduces the cumbersome process of authentication and achieves a fast authentication. The contributions of this paper include the following; 1) we design a decentralized authentication for V2R communication, 2) our proposed scheme uses continuously updated information for authentication, which guarantees that the AV can drive continuously without needing to stop for key updates, and 3) our proposed scheme ensures that all transmitted messages are dynamic and confidential and thus able to resist potential attacks.

II. RELATED WORKS

In recent decades, many studies have proposed designs for authentication schemes for secret communication across VSNs. Although the security and privacy challenges in VSNs are significant, Zaidi *et al.* [4] have claimed that the benefits of VSNs outweigh the associated risks, and should not thus limit their development. However, it is still important that research takes place in order to minimize security and privacy risks. Manvi and Tangade [6] have summarized authentication schemes for VSNs by classifying them into group employing cryptography techniques, digital signatures, or messages verification techniques. They claim that new authentication schemes should provide low computation and communication overheads while using decentralized authentication in the absence of a trusted third party. Some studies have focused on the traffic management system of VSNs. Wang *et al.* proposed a city-wide real-time traffic management system that enabled crowdsensing in social VSNs. With the objective of providing timely responses in heterogeneous social VSNs for traffic management, they proposed a crowdsensing-based real-time traffic management framework in a fully distributed manner and demonstrated that their framework is more effective than others [9]. In order to minimize the average response time for events reported by vehicles, Wang *et al.* [10] also proposed a feasible solution that enables offloading for real-time traffic management in fog-based VSNs and were the first authors to model parked and moving vehicle-based fog nodes by employing queueing theory. Their traffic management approach is advanced and effective. Chuang and Lee's scheme incorporates a hash chain as the secret key for the OBU [8] and law executors to authenticate mobile vehicles. When the vehicle is authenticated, the status of the vehicle is designated as trusted, and the scheme requires that only trusted vehicles can communicate with each other. Although their approach is able to achieve the anonymity of U and can resist the tracing attack, Zhou *et al.* [7] point out that their scheme is vulnerable to internal attack due to the sharing of a secret key. To overcome this vulnerability, Zhou *et al.* [7] proposed an enhanced privacy-preserving authentication scheme for VSNs that uses a hash chain and Elliptic Curve Computational (ECC) algorithm to protect the identity of U and the secret SK of communication while improving overall performance. However, Zhou *et al.*'s scheme is vulnerable to replay and malicious authenticated vehicle attacks and in their paper, only the computation overhead of the scheme was analyzed, and not the communication overhead. The AV must stop for key update due to the short period of the hash chain.

Kumar *et al.* [11] proposed a certificateless aggregate signature scheme for VSNs that requires a short bandwidth. Their scheme is unforgeable against adaptive chosen-message attacks and has a lower computational overhead compared to other schemes. Kumari *et al.* [12] proposed an enhanced and secure trust-extended authentication mechanism for VSNs which also uses a hash chain with a scheme that has a key update phase and a pseudo identity that is dynamic. Their scheme can resist various attacks including the tracing attack and insider attack, has a very low computation load and is more proficient than others.

Mohit *et al.* [13] proposed an authentication scheme to improve the security performance of VSNs using two sets of communications between the user and sink node and the sink node and sensor. This scheme only uses a hash function to achieve security of authentication, and the authors claim that the approach resists various attacks with low computational and communication overheads. However, their scheme does not include the V2V communication and smart card revocation phases. As the transmitted message and the secret key of the sink node are constant, the scheme remains vulnerable to tracing attack. Liu *et al.* [14] proposed an efficient and privacy-preserving dual authentication and key agreement scheme for secure V2V communications.

Their approach adopts a bilinear pairing to compute the encryption key and with this approach, vehicles can establish SK without knowing each other's real identity. Although their scheme can resist various attacks, it remains vulnerable to a malicious authenticated vehicle attack and cannot guarantee the integrity and non-repudiation of the message. Since the bilinear pairing operation is complicated, the overhead associated with computation and communication is very high. Azees *et al.* [15] proposed a means of efficient anonymous authentication with a conditional privacy-preserving scheme for VSNs that uses bilinear pairing encryption to enhance the security performance and to achieve the anonymity between the RSU and OBU. Although this scheme resists the malicious authenticated vehicle attack and achieves anonymity, it is unable to provide the smart card revocation phase and suffers from a high cost in terms of computational overhead due to the bilinear pairing operation. Vijayakumar *et al.* [16] proposed a computationally efficient privacy-preserving authentication and key distribution technique for VSNs. This approach avoids communications with malicious vehicles, achieves anonymity of RSUs and OBUs, and resists various attacks. However, this approach remains vulnerable to the tracing attack as well as the privileged insider and replay attacks. Their scheme also carries a significant overhead cost due to the bilinear pairing operation while the communication overhead was not addressed. Li *et al.* [17] proposed an anonymous conditional privacy-preserving authentication for VSNs and the authors also suggested the design goals of VSNs. Their scheme is efficient and adopts pseudo-identity generation and private key extraction to protect privacy. To reduce overhead, Zhong *et al.* [18] proposed a conditional privacy-preserving authentication scheme which adopts the registration list instead of the revocation list and it not use complicated computational operations; however, their scheme lacks V2V communication. As the registration time of the OBU is constant, their scheme is vulnerable to the tracing attack. Li *et al.* [19] proposed a security enhanced, identity-based and certificateless public key authentication scheme for VSNs which uses certificateless public key cryptography to address the disadvantages of certificate distribution while resisting the impersonation, stolen smart card, and replay attacks. However, their scheme is unable to provide a smart card revocation phase and remains vulnerable to malicious authenticated attack. Chen *et al.* [20] proposed a secure mutual authentication scheme with non-repudiation for vehicular ad hoc networks that adopts asymmetric message encryption and includes a secret key update phase. They claim that the scheme resists various attacks and achieve the security requirements of VSNs, however, it remains vulnerable to the replay, malicious authenticated vehicle, and tracing attacks, is unable to provide anonymity for the U, and, once again, the authors do not include an analysis of the communication overhead.

To design a decentralized authentication scheme in order to achieve fast-authentication, Wang *et al.* [21] proposed a vehicular ad hoc network privacy protection scheme without a trusted third party. They claim that a central authority is the cause of many security problems, and as a result their scheme offers decentralization for the privacy protection of the OBU in VSNs. Although this approach avoids the cumbersome process of authentication, it remains vulnerable to the stolen vehicle attack. It also suffers from a high computational overhead due to its modular exponentiation operations. Wang and Yao [22] proposed a local identity-based anonymous message authentication protocol in VSNs, which achieves the required authentication for the V2R communications without a trusted third party. Although they claim that their scheme achieves security and privacy for VSNs, it remains vulnerable to the malicious authenticated and tracing attacks and, whilst the computational overhead is analyzed, the communication overhead is not.

In addition to these authentication schemes, several advanced algorithms are also used in VSNs for security purposes. Tian and Qiang [23] proposed a signature scheme based on a proxy multi-signature and blind signature, and whilst their scheme has a good performance in terms of safety and efficiency, Wang *et al.* point out that it is vulnerable to attacks on privacy, conditional tracking, and distributed tracking. In order to solve these issues, Wang *et al.* [24] proposed a scheme based on a fair blind signature and a secret sharing algorithm. Their algorithm meets the privacy protection requirement and avoids the anonymous abuse. Compared with Xu and Song's scheme, the scheme of Wang *et al.* can resist various attacks and can reduce the average length of a message. Kumar *et al.* [25] proposed an intelligent approach to building a secure decentralized public key infrastructure in VSNs using advanced algorithms to reward or penalize players' actions. Upon receiving feedback, players update the probability vector of actions and decide on a strategy. With the increasingly stringent requirement of a response time, several studies are focused on reducing the response time of vehicles. As a vehicle moves fast on the road, reducing the response time is of practical use for VSNs.

Ning *et al.* [26] proposed a cooperative partial computation offloading scheme for Internet of Things. They designed an iterative heuristic mobile edge computing resource allocation scheme to solve the multi-user computation offloading problem which reduces execution delay by 30 per cent. As the resources of the OBU are not constrained, their scheme is suitable for VSNs. Wang *et al.* [27] proposed a privacy-preserving message forwarding framework for an opportunistic cloud of Things, which protects privacy and improves transmission efficiency. An attribute-based cryptographic algorithm is integrated into a message delivery process to resist attacks. Ning *et al.* [28] proposed a green and sustainable cloud of Things: enabling collaborative edge computing. They adopt a reliability function to confirm the number of backup edge devices with the aim of minimizing the response time of citywide events collected and reported by vehicles, Ning *et al.* [29] proposed a method of vehicular fog computing: enabling real-time traffic management for

TABLE 1. Notations in our paper.

Abbreviation	Description
U	User, who is the driver of vehicle
RSUs	Roadside units deployed along the roadside
OBUs	Onboard units which is deployed in AV
TA	Trusted authority
VSNs	Vehicle Sensor Networks
AV	Autonomous vehicle
SC	The smart card of U
$\mathcal{A}$	The adversary, who can attack on the VSNs
ID_{SC}, ID_i, ID_V	The identity of SC, driving license number of U, and identification number of AV, respectively
PW_i	The password of U
BIO_i	The biometric feature of U
L_n	The location number of VSNs
st	The continuously updated information
TS	The timestamp
RN	The random number
$Gen(\cdot)/Rep(\cdot)$	The fuzzy extractor generation/reproduction algorithm
$h(\cdot)$	Hash function
$HMAC_k(\cdot)$	Hash Message authentication code function with the secret key k
$Ver_k(\cdot)$	Verify function with the secret key k
$D_k(\cdot)/E_k(\cdot)$	Symmetrical decryption/encryption algorithm with the secret key k
Z_p^*	The set consisting of all primes in $\{0,1,\cdots,p-1\}$
$\|$	Bitwise concatenation operation
$\oplus$	XOR operation

smart cities, they construct a three-layer vehicular fog computing model for distributed traffic management.

III. PRELIMINARIES

A. NOTATIONS OF OUR PAPER

The used notations of this paper are described in Table 1.

B. NETWORK MODEL FOR VSNs

VSNs typically consist of three entities: OBU, which is a semi-trusted unit deployed in the AV, RSU, which is a trusted node deployed on the roadside, and the TA, which is the trusted third party for the VSN [18]. According to [6], [7], and [18], the RSUs and TA form a secure area network via wires and cables and can share both traffic and authentication-related information from the OBU with each other in real-time. The OBU communicates with the RSU and other OBUs via an unsafe wireless channel [30] and the TA is responsible for verifying the legality of the U and AV and for the registration of OBU. After registration, the TA broadcasts the

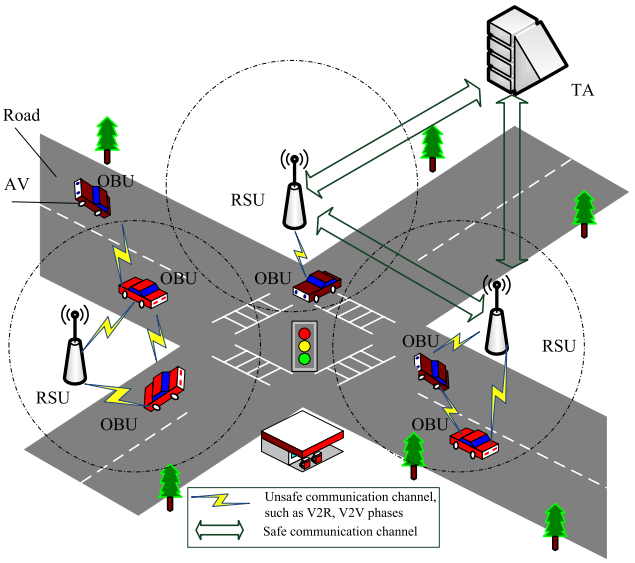

FIGURE 1. Network model for autonomous vehicle networks.

information to all RSUs via a secure channel. The times and locations through a geographic region number for the entire VSN are synchronized. The TA and RSUs have large computation and storage capabilities and a broad communication coverage area. Some functional devices can be included and mounted onto the cars, such as smart card readers and biometric extraction devices. Once the RSU authenticates the OBU, the status of the OBU changes to a trusted vehicle. In real environments, VSNs only require that the trusted vehicle can communicate with other vehicles via the wireless channel, enabling a safe environment [7]. The network model for VSNs is presented in Fig.1.

C. THE CAPABILITIES OF THE ADVERSARY

The potential capabilities of the adversary, $\mathcal{A}$, include the followings:

1. Intercept, modify, and replay transmitted messages via the VSNs [31].
2. Guess the cryptographic nonce with a probability of approximately $\frac{1}{2^{6n}}$ for a nonce with n characters [32].
3. Comprise the SC and AVs as it is possible for $\mathcal{A}$ to obtain the information stored in the memory of the SC with a powerful analysis attack [33]. This allows $\mathcal{A}$ to hack into a single OBU_i in order to obtain the stored information via other methods [34]. Then, the authenticated vehicle can maliciously impersonate other legal AVs with the information retrieved.

IV. OUR PROPOSED SCHEME

Our scheme adopts temporary and confidential updated information and a dynamic secret key to resist the tracing attack and to achieve mutual authentication between an OBU_i and RSU_i. As the information is held temporarily and is confidential, this innovation means that the scheme is untraceable and overcomes the vulnerability of the hash chain, which latter only offers a short lifetime for the secret key.

It also guarantees that AVs can run on the road continuously as it is unnecessary for the AV to stop for a key update. At the end of the authentication phase, the OBU_i and RSU_i negotiate a temporary SK, which is more secure than long-term keys [35], and update the authenticated information simultaneously. When the mutual authentication is complete, the RSU_i broadcasts the updated information to all RSUs via a secure channel and the status of the vehicle is designated as trusted. Only the trusted vehicle can communicate with other vehicles. As our proposed scheme consists of a series of calculations and the time complexity of the hash, HMAC, and symmetrical decryption/encryption are linear, the time complexity of our proposed scheme is the same as that of a fuzzy extractor generation/reproduction algorithm which is $O(n^3)$ [36]. Our proposed scheme consists of seven phases: system setup, registration for the user, login, authentication and key agreement, update, smartcard revocation, and V2V communication. The single arrow line and double solid lines used in the following figures represent an unsafe and a safe communication channel, respectively.

A. SYSTEM SETUP PHASE

Before the AV operates on the road, it is essential to embed the base functions into the SCs, OBUs, RSUs, and TA within a rigorously secure environment.

1. All legitimate ID_{SC}, ID_i, and ID_V must be registered in the TA.

2. Then TA embeds Z_p^*, P, n, XOR, h(·), ||, $HMAC_k$ (Mac, Ver), Global Positioning System (GPS), and geographic regions number sets of the VSNs into the memory of the OBUs, RSUs, and TA.

B. REGISTRATION PHASE FOR THE USER

Before the AV operates on the road, the driver and OBU_i must be registered in the TA via a secure channel and the presented in Fig. 2 are executed.

1. U inserts SC and inputs his driving license number ID_i in OBU_i. Then OBU_i retrieves ID_{SC} and vehicle identification number ID_V. Finally, OBU_i sends $\{ID_i, ID_V, ID_{SC}\}$ to TA.

2. TA checks whether ID_V, ID_i, and ID_{SC} are legal. If they are illegal, TA rejects the request. Otherwise, TA sends the confirmation message to OBU_i.

3. Upon receiving the message, OBU_i agrees U to register in TA. Then U inputs password PW_i and his biometric feature BIO_i in the biometric extraction device. SC generates a random number RN_i and computes $(\sigma_i, \tau_i) = Gen(BIO_i)$, $CN_i = RN_i \oplus h(ID_{SC} \| ID_V \| ID_i \| \sigma_i \| PW_i)$, $RPW = h(RN_i \| \sigma_i \| PW_i \| ID_i)$. Finally SC gets the current timestamp TS_1 and sends $\{RPW, TS_1, RN_i\}$ to TA via the secure channel.

4. Upon receiving message, TA first checks the freshness of TS_1. If it is not fresh, TA rejects the registration request. Otherwise, TA generates random numbers d and $x \in Z_p^*$. Then TA gets the geographic number L_n, timestamp TS_2 and computes, $PSK^{old} = h(x)$, $TC_i = h(d \| RN_i \| ID_V)$, $st^{old} = h(TS_2 \| \_i \| \_x)$, $PD = d \oplus h(RN_i \| RPW)$,

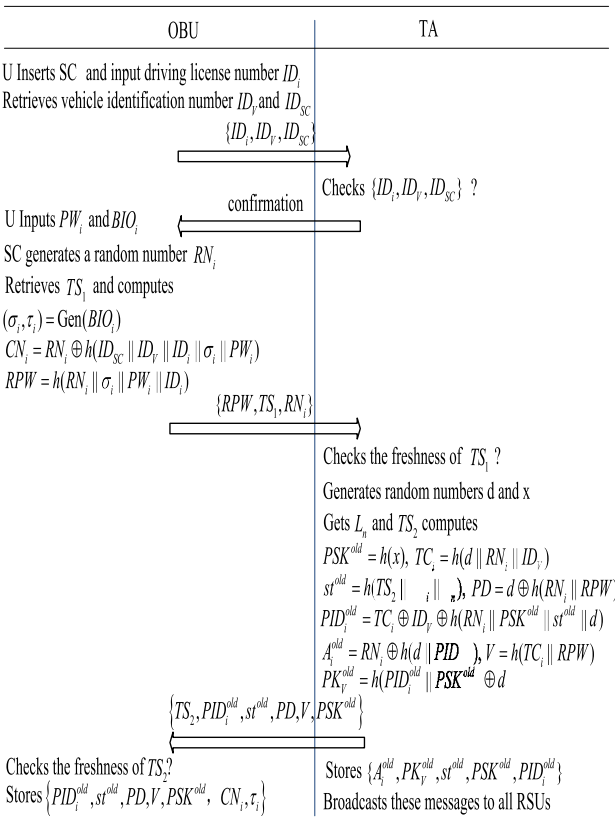

FIGURE 2. Registration phase for user.

$PID_i^{old} = TC_i \oplus ID_V \oplus h(RN_i \| PSK^{old} \| st^{old} \| d)$, $V = h(TC_i \| RPW)$, $A_i^{old} = RN_i \oplus h(d \| PID_i^{old})$, and $PK_V^{old} = h(PID_i^{old} \| PSK^{old}) \oplus d$. Then TA transmits $\{TS_2, PID_i^{old}, st^{old}, PD, V, PSK^{old}\}$ to OBU_i. Finally, TA stores $\{A_i^{old}, PK_V^{old}, st^{old}, PSK^{old}, PID_i^{old}\}$ and broadcasts these messages to all RSUs which are deployed along the roadside via a secure channel.

5. OBU_i checks the freshness of TS_2. If it is not fresh, OBU_i aborts the session. Otherwise, OBU_i stores $\{PID_i^{old}, CN_i, \tau_i, PD, st^{old}, PSK^{old}, V\}$ into the memory.

C. LOGIN PHASE

It is necessary for OBU_i to verify the legality of the driver before joining the VSNs, as described in Fig. 3.

1. U inserts his assigned SC, inputs driving license number ID_i, password PW_i, and imprints BIO_i at the terminal device.

2. OBU_i retrieves ID_{SC}, ID_V and computes $\sigma_i = Rep(BIO_i, \tau_i)$, $RN_i = h(ID_{SC} \| ID_V \| ID_i \| \sigma_i \| PW_i) \oplus CN_i$, $RPW = h(RN_i \| \sigma_i \| PW_i \| ID_i)$, $d = PD \oplus h(RN_i \| RPW)$, $TC_i = PID_i^{old} \oplus ID_V \oplus h(RN_i \| PSK^{old} \| st^{old} \| d)$, $V^* = h(TC_i \| RPW)$.

3. OBU_i checks whether $V^* = V$?. If it is not equal, OBU_i rejects the login request. Otherwise, OBU_i generates a random number α and gets the current timestamp TS_1, then OBU_i computes $PA = \alpha \oplus h(TS_1 \| TC_i \| PSK^{old} \|$

d ‖ RN_i), $DID_V = ID_V \oplus h(TS_1 \| d \| PSK^{old} \| RN_i)$, $C_{OBU} = HMAC_\alpha(PA \| TS_1 \| DID_V \| st^{old} \| TC_i \| RN_i)$. Finally, OBU_i transmits $\{C_{OBU}, PA,, DID_V, TS_1, PID_i^{old}\}$ to RSU_i via a wireless channel.

D. AUTHENTICATION AND KEY AGREEMENT PHASE

When the AV is driving into the range of a new RSU_i, the RSU_i and OBU_i must achieve mutual authentication and negotiate for the temporary SK. When the authentication and key agreement phase is complete, the status of the AV switches to trusted. If the TA detects that RSU_j is compromised, then the TA notifies other RSUs that RSU_j is invalid. The legitimate RSUs encrypt this information with the SK and send it to the authenticated vehicles to prevent further communication between RSU_j and the vehicles. This phase is presented in Fig.3.

1. Upon receiving this message, RSU_i checks the freshness of TS_1. If it is not fresh, RSU_i aborts the session. Otherwise, RSU_i obtains $\{A_i^{old}, PK_V^{old}, st^{old}, PSK^{old}\}$ corresponding to PID_i^{old}, and computes $d = PK_V^{old} \oplus h(PID_i^{old} \| PSK^{old})$, $RN_i = A_i^{old} \oplus h(d \| PID_i^{old})$, $ID_V = DID_V \oplus h(TS_1 \| d \| PSK^{old} \| RN_i)$, $TC_i = h(d \| RN_i \| ID_V)$, $\alpha = PA \oplus h(TS_1 \| TC_i \| PSK^{old} \| d \| RN_i)$. Then RSU_i checks whether $Ver_\alpha(PA \| TS_1 \| DID_V \| st^{old} \| TC_i \| RN_i, C_{OBU}) = 1$? If it is not equal, RSU_i aborts the session. Otherwise, RSU_i retrieves TS_2 and generates a random number β. RSU_i computes $PB = \beta \oplus h(TS_2 \| d \| st^{old} \| RN_i \| TC_i)$, $SK = h(\alpha \| \beta \| PSK^{old} \| st^{old})$, and $C_{RSU} = HMAC_\beta(PB \| SK \| TC_i \| TS_2 \| RN_i)$. Finally, RSU_i sends $\{C_{RSU}, TS_2, PB\}$ to OBU_i.

2. Upon receiving this message, OBU_i checks the freshness of TS_2. If it is not fresh, OBU_i aborts the session. Otherwise, OBU_i computes $\beta = PB \oplus h(TS_2 \| d \| st^{old} \| RN_i \| TC_i)$ and $SK = h(\alpha \| \beta \| PSK^{old} \| st^{old})$. Then OBU_i checks whether $Ver_\beta(PB \| SK \| TC_i \| TS_2 \| RN_i, C_{RSU}) = 1$? If it is not equal, OBU_i aborts the session. Otherwise, OBU_i retrieves TS_3 and sends the confirmation message to RSU_i, which is encrypted with SK. Then OBU_i retrieves the geographic number L_n^{new} of RSU_i and updates PSK^{old} with $PSK^{new} = h(PSK^{old})$, st^{old} with $st^{new} = h(TS_2 \| TC_i \| L_n^{new})$, and PID_i^{old} with $PID_i^{new} = TC_i \oplus ID_V \oplus h(RN_i \| PSK^{new} \| st^{new} \| d)$. Finally, the status of AV changes to trusted vehicle.

3. Upon receiving the message, RSU_i checks the freshness of TS_3. If it is fresh, RSU_i decrypts the message with SK to obtain the confirmation message, then RSU_i retrieves the new geographic number L_n^{new} of RSU_i and updates PSK^{old} with $PSK^{new} = h(PSK^{old})$, st^{old} with $st^{new} = h(TS_2 \| TC_i \| L_n^{new})$, PID_i^{old} with $PID_i^{new} = TC_i \oplus ID_V \oplus h(RN_i \| PSK^{new} \| st^{new} \| d)$, A_i^{old} with $A_i^{new} = RN_i \oplus h(d \| PID_i^{new})$, and PK_V^{old} with $PK_V^{new} = h(PID_i^{new} \| PSK^{new}) \oplus d$. Finally, RSU_i broadcasts the updated authentication information $\{A_i^{new}, PK_V^{new}, st^{new}, PSK^{new}, PID_i^{new}\}$ via the secure channel. Upon receiving the continuously updated information, all RSUs update the stored information for next authentication.

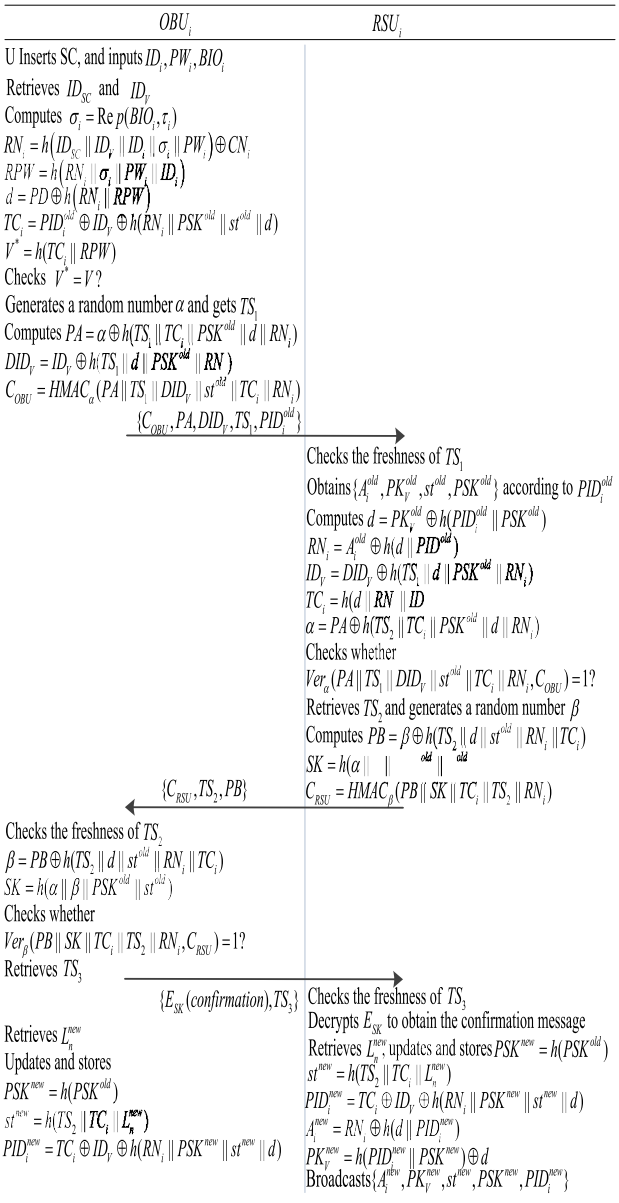

FIGURE 3. Login and authentication phase.

E. UPDATE PHASE

In real environments, it is important for U to change their login information periodically for safety considerations, and this can be accomplished with the help of the OBU_i and RSU_i. This functional portion of our scheme is described in the following phase.

1. The first step of this phase is to verify the legality of U. It is executed the same steps as the login, authentication and key agreement phase until the temporary secret key SK is negotiated between OBU_i and RSU_i. If U passes the verification, OBU_i agrees U to update his login information. Otherwise, OBU_i rejects the update request.

2. U inputs new password PW_i^* and his new biometric feature BIO_i^* in the biometric extraction device. Then

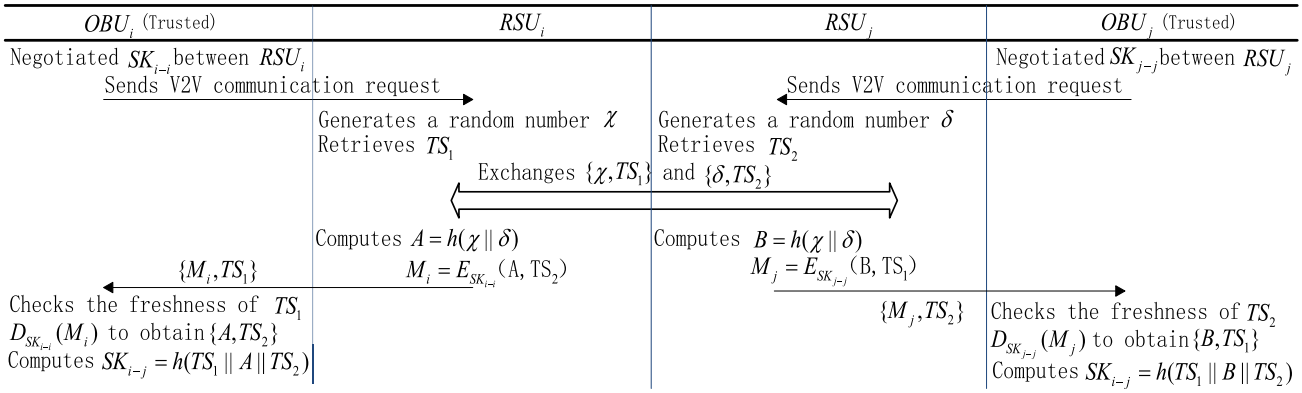

FIGURE 4. Vehicle-to-vehicle key agreement phase.

SC generates a new random number RN_i^*, retrieves TS_1 and computes $(\sigma_i^*, \tau_i) = Gen(BIO_i^*)$, $CN_i^* = RN_i^* \oplus h(ID_{SC} \| ID_V \| ID_i \| \sigma_i^* \| PW_i^*)$, $RPW^* = h(RN_i^* \| \sigma_i^* \| PW_i^* \| ID_i)$, and $M_1 = E_{SK}(RPW^*, TS_1, RN_i^*, ID_V)$. Then OBU_i sends $\{M_1, TS_1\}$ to RSU_i.

3. Upon receiving the message, RSU_i first checks the freshness of TS_1. If it is not fresh, RSU_i rejects the request. Otherwise, RSU_i decrypts M_1 to obtain $\{RPW^*, TS_1, RN_i^*, ID_V\}$ with SK, generates new random numbers $d^*, x^* \in Z_p^*$, gets the geographic number L_n^*, and retrieves TS_2. Then RSU_i computes $PSK^* = h(x^*)$, $TC_i^* = h(d^* \| RN_i^* \| ID_V)$, $st^* = h(TS_2 \| TC_i^* \| L_n^*)$, $PD^* = d^* \oplus h(RN_i^* \| RPW^*)$, $PID_i^* = TC_i^* \oplus ID_V \oplus h(RN_i^* \| PSK^* \| st^* \| d^*)$, $V^* = h(TC_i^* \| RPW^*)$, $A_i^* = RN_i^* \oplus h(d^* \| PID_i^*)$, $PK_V^* = h(PID_i^* \| PSK^*) \oplus d^*$, $M_2 = E_{SK}(TS_2, PID_i^*, st^*, PD^*, V^*, PSK^*)$. Finally RSU_i transmits $\{M_2, TS_2\}$ to OBU_i. Then RSU_i stores and broadcasts $\{A_i^*, PK_V^*, st^*, PSK^*, PID_i^*\}$ to all RSUs which are deployed along the roadside via a secure channel.

4. Upon receiving the message, OBU_i checks the freshness of TS_2. If it is not fresh, OBU_i rejects the request. Otherwise, OBU_i decrypts M_2 to get $\{TS_2, PID_i^*, st^*, PD^*, V^*, PSK^*\}$. Then OBU_i updates $\{PID_i^*, CN_i^*, \tau_i, PD^*, st^*, PSK^*, V^*\}$ into the memory.

F. SMART CARD REVOCATION PHASE

As the SC of the U may be lost or damaged, it is necessary to incorporate a smart card revocation phase to invalidate the SC for safety considerations. In our scheme, only the system administrator (SA) can cancel the SC and assign a new SC to U. The SA has the right to cancel the SC and login into the OBU_i via a direct cable connection. This functional portion of our scheme is described in the following phase.

1. SA logins into the OBU_i locally and obtains PID_i^{old} from the memory of OBU_i, then SA deletes the stored authentication information of OBU_i corresponding to PID_i^{old}.

2. SA sends the lost temporary identity PID_i^{old} to all RSUs via the secure channel. Upon receiving deleted message form SA, RSUs delete the authentication information which is corresponding to PID_i^{old}.

3. SA registers new SC in TA and assigns the new SC to U. Then the rest of steps are the same as the registration phase for U.

G. VEHICLE-TO-VEHICLE KEY AGREEMENT PHASE

In real environments, vehicles need to interact and thus secret communication must be established between the OBU_i and OBU_j. Our scheme requires that only trusted vehicles can communicate through a V2V secret communication channel that is established with the assistance of the RSU. We assume OBU_i is operating within the communication range of RSU_i and OBU_j is within the communication range of RSU_j. This phase is presented in Fig.4.

1. OBU_i and OBU_j must be authenticated by RSU_i and RSU_j until the status of AV changes to trusted. When the authentication phase is completed, the temporary SK_{i-i} and SK_{j-j} between OBU_i and RSU_i, OBU_j and RSU_j are negotiated.

2. If the trusted vehicles want to share the public information, such as road condition, speed, vehicle condition etc., OBU_i and OBU_j broadcast public information in plaintext to all AVs which are running on the road via the public channel. Otherwise, the secure communication channel must be established between OBU_i and OBU_j.

3. OBU_i sends V2V communication request to RSU_i, OBU_j sends V2V communication request to RSU_j. Upon receiving the request, RSU_i generates a random number χ and retrieves TS_1. RSU_j generates a random number δ and retrieves TS_2. Then RSU_i exchanges $\{\chi, TS_1\}$ and $\{\delta, TS_2\}$ with RSU_j via the secure channel. RSU_i computes $A = h(\chi \| \delta)$ and $M_i = E_{SK_{i-i}}(A, TS_2)$, RSU_j computes $B = h(\chi \| \delta)$ and $M_j = E_{SK_{j-j}}(B, TS_1)$. Finally, RSU_i sends $\{M_i, TS_1\}$ to OBU_i and RSU_j sends $\{M_j, TS_2\}$ to OBU_j.

4. Upon receiving these messages, OBU_i and OBU_j first check the freshness of TS_1 and TS_2. If they are not fresh, OBU_i and OBU_j reject the request. Otherwise, OBU_i decrypts

M_i to obtain $\{A,TS_2\}$ with SK_{i-i} and OBU_j decrypts M_j to obtain $\{B,TS_1\}$ with SK_{j-j}. Then OBU_i computes $SK_{i-j} = h(TS_1 \| A \| TS_2)$ and OBU_j computes $SK_{i-j} = h(TS_1 \| B \| TS_2)$. Finally, the secret key SK_{i-j} between OBU_i with OBU_j is negotiated, and they can communicate secretly with the key SK_{i-j}.

5. If one of OBU_i and OBU_j is running into the range of new RSU_i or RSU_j, this phase must be executed again and the new SK between OBU_i and OBU_j must be negotiated again.

V. SECURITY ANALYSIS

We apply formal and informal methods to the analysis of the security performance of our proposed scheme. During the V2V key agreement phase, and since the communication channel between RSU_i and RSU_j is secure, RSU_i and RSU_j can be regarded as a single communication entity. Through a detailed analysis, we have determined that our scheme can withstand several forms of attack. We apply Burrow-Abadi-Needham logic (BAN-logic) to analyze the correctness of the authentication scheme and the V2V key agreement phase, a means which is widely used and accepted [37]. BAN-logic is a well-known formal logic to analyze whether the SK between participants is negotiated secretly, and uses a series of logic rules to verify the source, trustworthiness, and freshness of the transmitted message in the scheme.

A. CORRECTNESS ANALYSIS USING BAN-LOGIC

1) PRELIMINARIES AND NOTATIONS OF BAN-LOGIC

The preliminaries of BAN-logic are defined as follows:

P: denotes the principal, X and Y denote the statements.

P$|\equiv$ X: P believes X. P believes X or P would be entitled to believe X. P can take X as true.

P $\triangleleft$ X: P sees X. Someone has sent a message containing X to P, who can read and repeat X.

P$|\sim$ X: P once said X. P sent a message including the statement X and it is not known whether the message is fresh or not, however, it is known P believed X when P sent it.

P $\Rightarrow$ X: P has jurisdiction over X. P is an authority on X and should be trusted on this matter.

#(X): The message including X is fresh.

(X, Y): The formulae X or Y is one part of the formulae (X, Y).

$<$ X $>_Y$: X combined with Y.

$\{X\}_K$: X is encrypted under the key K.

$(X)_K$: X is hashed with the key K.

P $\overset{K}{\leftrightarrow}$ Q: P and Q communicate via shared secret key K.

K: The secret session key between P and Q. K never be obtained by any principal except P or Q.

P $\overset{X}{\Leftrightarrow}$ Q: The formulae X is only known to P and Q. X can be used by P and Q to prove identities.

Rules: The following rules are main rules used in BAN logic:

The Message-meaning rule: $\frac{P|\equiv P\overset{K}{\leftrightarrow}Q, P\triangleleft\{X\}_K}{P|\equiv Q|\sim X}$, $\frac{P|\equiv P\overset{Y}{\Leftrightarrow}Q, P\triangleleft<X>_Y}{P|\equiv Q|\sim X}$

If P believes that the secret key K is shared with Q and sees X encrypted under K, then P believes that Q once said X.

The nonce-verification rule: $\frac{P|\equiv\#(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$

If P believes the message or formulae X is fresh and Q once said X, then P believes that Q believes X.

The jurisdiction rule: $\frac{P|\equiv Q\Rightarrow X, P|\equiv Q|\equiv X,}{P|\equiv X}$

If P believes that Q has jurisdiction over X and P believes that Q believes X, then P believes X.

The belief rule: $\frac{P|\equiv X, P|\equiv Y,}{P|\equiv(X,Y)}$ $\frac{P|\equiv(X,Y)}{P|\equiv X}$, $\frac{P|\equiv Q|\equiv(X,Y)}{P|\equiv Q|\equiv X}$

If P believes X and Y, then P believes (X, Y). If P believes (X, Y), then P believes X or Y. If P believes that Q believes (X, Y), then P believes that Q believes X or Y.

The freshness rule: $\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$

If one part of formulae X is fresh, then the entire formulae (X, Y) must be fresh.

The session key rule: $\frac{P|\equiv\#(X), P|\equiv Q|\equiv X}{P|\equiv P\overset{K}{\leftrightarrow}Q}$

If P believes X is fresh and P believes that Q believes X, which is the necessary parameters of K, then P believes that P shares the secret K with Q.

2) THE SECURITY GOALS

Goal 1. $RSU_i| \equiv OBU_i \overset{SK}{\leftrightarrow} RSU_i$

Goal 2. $RSU_i| \equiv OBU_i| \equiv OBU_i \overset{SK}{\leftrightarrow} RSU_i$

Goal 3. $OBU_i| \equiv RSU_i \overset{SK}{\leftrightarrow} OBU_i$

Goal 4. $OBU_i| \equiv RSU_i| \equiv RSU_i \overset{SK}{\leftrightarrow} OBU_i$

Goal 5. $OBU_i| \equiv OBU_j \overset{SK_{i-j}}{\longleftrightarrow} OBU_i$

Goal 6. $OBU_i| \equiv OBU_j| \equiv OBU_j \overset{SK_{i-j}}{\longleftrightarrow} OBU_i$

Goal 7. $OBU_j| \equiv OBU_i \overset{SK_{i-j}}{\longleftrightarrow} OBU_j$

Goal 8. $OBU_j| \equiv OBU_i| \equiv OBU_i \overset{SK_{i-j}}{\longleftrightarrow} OBU_j$

3) THE IDEALIZED INITIAL STATUS FORMS OF OUR PROPOSED SCHEME

A_1: $OBU_i| \equiv \#(\alpha, \beta, PSK^{old})$

A_2: $RSU_i| \equiv \#(\alpha, \beta, PSK^{old})$

A_3: $OBU_i| \equiv \#(TS_1, TS_2, A)$

A_4: $OBU_j| \equiv \#(TS_1, TS_2, B)$

A_5: $OBU_i| \equiv OBU_i \overset{d}{\leftrightarrow} RSU_i$

A_6: $OBU_j| \equiv OBU_j \overset{SK_{j-j}}{\longleftrightarrow} RSU_j$

A_7: $OBU_i| \equiv OBU_i \overset{SK_{i-i}}{\longleftrightarrow} RSU_i$

A_8: $RSU_i| \equiv RSU_i \overset{d}{\leftrightarrow} OBU_i$

A_9: $OBU_i \triangleleft \{OBU_i \overset{A}{\leftrightarrow} OBU_j\}_{SK_{i-i}}$

A_{10}: $OBU_j \triangleleft \{OBU_i \overset{B}{\leftrightarrow} OBU_j\}_{SK_{j-j}}$

A_{11}: $OBU_i \triangleleft \{\alpha\}_d$

A_{12}: $RSU_i \triangleleft \{\alpha\}_d$

A_{13}: $RSU_i \triangleleft \{OBU_i \overset{\alpha}{\leftrightarrow} RSU_i\}_d$

A_{14}: $OBU_i| \equiv RSU_i \Longrightarrow OBU_i \overset{A}{\leftrightarrow} OBU_j$

A_{15}: $OBU_j| \equiv RSU_j \Longrightarrow OBU_i \overset{B}{\leftrightarrow} OBU_j$

A_{16}: $OBU_i \triangleleft \{RSU_i \overset{\alpha}{\leftrightarrow} OBU_i\}_d$

4) THE IDEALIZED TRANSFORMED MESSAGES OF OUR SCHEME

M_1: $OBU_i \rightarrow RSU_i$:{C_{OBU}, PA, DID_V, TS_1, PID_i^{old}}
M_2: $RSU_i \rightarrow OBU_i$:{C_{RSU}, TS_2, PB}
M_3: $RSU_i \rightarrow OBU_i$:{M_i, TS_1}
M_4: $RSU_j \rightarrow OBU_j$:{M_j, TS_2}

5) THE MAIN ANALYSIS STEPS OF OUR PROPOSED SCHEME BASED ON BAN LOGIC

By A_8, A_{13}, and the message-meaning rule, we get:
S_1: $RSU_i| \equiv OBU_i| \sim OBU_i \overset{\alpha}{\leftrightarrow} RSU_i$
By A_2, S_1 and the nonce-verification rule which α is the necessary part of SK, we get:
S_2: $RSU_i| \equiv OBU_i| \equiv OBU_i \overset{SK}{\leftrightarrow} RSU_i$ (Goal 2)
By M_1 and the seeing rule, we get:
S_3: $RSU_i \triangleleft (C_{OBU}, PA, DID_V, TS_1, PID_i^{old})$
By A_8, S_3, A_{12} and the message-meaning rule, we get:
S_4: $RSU_i| \equiv OBU_i| \sim \alpha$
By S_4, A_2, freshness rule and nonce-verification, we get:
S_5: $RSU_i| \equiv OBU_i| \equiv \alpha$
By S_5, A_2, and session keys rule which α is the necessary part of SK, we get:
S_6: $RSU_i| \equiv OBU_i \overset{SK}{\leftrightarrow} RSU_i$ **(Goal 1)**
By A_{16}, A_5, and the message-meaning rule, we get:
S_7: $OBU_i| \equiv RSU_i| \sim RSU_i \overset{\alpha}{\leftrightarrow} OBU_i$
By A_1, S_7 and the nonce-verification rule which α is the necessary part of SK, we get:
S_8: $OBU_i| \equiv RSU_i| \equiv RSU_i \overset{SK}{\leftrightarrow} OBU_i$ **(Goal 4)**
By M_2 and the seeing rule, we get:
S_9: $OBU_i \triangleleft (C_{RSU}, TS_2, PB)$
By A_{11}, S_9, A_5 and the message-meaning rule, we get:
S_{10}: $OBU_i| \equiv RSU_i| \sim \alpha$
By A_1, S_{10}, freshness rule and nonce-verification, we get:
S_{11}: $OBU_i| \equiv RSU_i| \equiv \alpha$
By A_1, S_{11}, and the session keys rule which α is the necessary part of SK, we get:
S_{12}: $OBU_i| \equiv RSU_i \overset{SK}{\leftrightarrow} OBU_i$ **(Goal 3)**
By M_3, A_9, S_{12}, and message-meaning rule, we get:
S_{13}: $OBU_i| \equiv RSU_i| \sim OBU_i \overset{A}{\leftrightarrow} OBU_j$
By S_{13}, A_3, and nonce-verification rule, we get:
S_{14}: $OBU_i| \equiv RSU_i| \equiv OBU_i \overset{A}{\leftrightarrow} OBU_j$
By S_{14}, A_{14}, and jurisdiction rule, we get
S_{15}: $OBU_i| \equiv OBU_i \overset{A}{\leftrightarrow} OBU_j$
By S_{15}, which A is the necessary part of SK_{i-j}, we get:
S_{16}: $OBU_i| \equiv OBU_j \overset{SK_{i-j}}{\longleftrightarrow} OBU_i$ **(Goal 5)**
By S_{15}, A_9, and message-meaning rule, we get:
S_{17}: $OBU_i| \equiv OBU_j| \sim OBU_i \overset{A}{\leftrightarrow} OBU_j$
By S_{17}, A_3, and the nonce-verification rule which A is the necessary part of SK_{i-j}, we get:
S_{18}: $OBU_i| \equiv OBU_j| \equiv OBU_i \overset{SK_{i-j}}{\longleftrightarrow} OBU_j$ **(Goal 6)**
By M_4, A_{10}, S_{12}, and message-meaning rule, we get:

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/
results/hlpslGenFile.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.01s
  visitedNodes: 9 nodes
  depth: 4 plies
```

FIGURE 5. Simulated result in OFMC back-end.

S_{19}: $OBU_j| \equiv RSU_j| \sim OBU_i \overset{B}{\leftrightarrow} OBU_j$
By S_{19}, A_5, and nonce-verification rule, we get:
S_{20}: $OBU_j| \equiv RSU_j| \equiv OBU_i \overset{B}{\leftrightarrow} OBU_j$
By S_{20}, A_{15}, and jurisdiction rule, we get
S_{21}: $OBU_j| \equiv OBU_i \overset{B}{\leftrightarrow} OBU_j$
By S_{21}, which B is the necessary part of SK_{i-j}, we get:
S_{22}: $OBU_j| \equiv OBU_j \overset{SK_{i-j}}{\longleftrightarrow} OBU_i$ **(Goal 7)**
By S_{21}, A_{10}, and message-meaning rule, we get:
S_{23}: $OBU_j| \equiv OBU_i| \sim OBU_i \overset{B}{\leftrightarrow} OBU_j$
By S_{23}, A_4, and the nonce-verification rule which B is the necessary part of SK_{i-j}, we get:
S_{24}: $OBU_j| \equiv OBU_i| \equiv OBU_i \overset{SK_{i-j}}{\longleftrightarrow} OBU_j$ **(Goal 8)**
From the analysis above, our proposed scheme achieves all the security goals, which suggests our proposed scheme provides mutual authentication and negotiates temporary session keys between OBU_i and OBU_j as well as OBU_i and RSU_i safely.

B. SIMULATION OF PROPOSED SCHEME

In this section, we simulate our scheme using automated validation of internet security protocols and applications (AVISPA) tool which is widely-accepted for the formal verification to measure whether the scheme is correct and practicable [38]. AVISPA is a powerful modular and implement a variety of state-of-the-art automatic analysis techniques and various back-ends which are integrated through the HLPSL (High Level Protocols Specification Language). Our scheme is simulated based on the widely-accepted OFMC back-end, which implements several correct and complete symbolic techniques. The simulation result is shown in Fig.5.

The simulation result confirms that our proposed scheme is correct and safe against active and passive attacks. Therefore, it is practical in real environments.

C. INFORMAL SECURITY ANALYSIS

1) MALICIOUS AUTHENTICATED VEHICLE ATTACK

In real environments, an authenticated vehicle may become malicious during an attack. In many schemes, the secret key d of the RSU is always the same and is widely used. According to the capabilities model for $\mathcal{A}$, if $\mathcal{A}$ is the authenticated vehicle, then it can obtain d of the RSU during the authentication phase. If d is also used to authenticate other vehicles, then $\mathcal{A}$ can intercept the transmitted message and decode the secret key from another AV using d. Therefore, $\mathcal{A}$ can impersonate other AVs to pass the verification phase and thereby obtain the SK from the transmitted message. In our proposed scheme, the secret key d of the RSU is different for each vehicles. Therefore, if the authenticated vehicle becomes malicious it is impossible for $\mathcal{A}$ to decode a message from another AV as the transmitted message is dynamic and encrypted by hash. According to the properties of hash, it is impossible for $\mathcal{A}$ to derive d in polynomial time. However, $\mathcal{A}$ may employ a guessing attack to determine d, although this has a negligible probability of success at $\frac{1}{2^{128+160+128}}$, where the length of the random numbers and hash output are 128 bits and 160 bits, respectively. Therefore, our scheme can withstand the malicious authenticated vehicle attack.

2) ANONYMITY

Anonymity is of great concern in authentication schemes conducted via wireless channels as it is essential to protect the privacy of U. In our scheme, we encrypt ID_V of the AV in DID_V with RN_i and PSK^{old}. If $\mathcal{A}$ can intercept DID_V via the wireless channel, since the PSK^{old} is dynamic, and RN_i is secret, it is impossible for $\mathcal{A}$ to derive ID_V from DID_V because of the hash function. However, $\mathcal{A}$ may attempt to guess the ID_V with a probability approximately equal to the negligible $\frac{1}{2^{6n+128+128+160}}$ where n represents ID_V with n characters, and the length of hash function and random number are 160 bits and 128 bits, respectively. Therefore, our proposed scheme can achieve anonymity of the U and OBU_i.

3) TRACKING ATTACK

According to the adversary model, $\mathcal{A}$ could intercept the transmitted message via the wireless channel and trace the vehicle by the constantly transmitted message. In our scheme, all transmitted information is dynamic and adopts temporary and confidential updated information, which is encrypted into PID_i^{old}. When the authentication is complete, the pseudo identity PID_i^{old} at both OBU_i and RSU_i are updated simultaneously, thereby making it impossible for $\mathcal{A}$ to trace OBU_i from the transmitted information. Therefore, our proposed scheme resists the tracing attack.

4) NON-REPUDIATION OF MESSAGE

In our proposed scheme, we use the HMAC function to validate the non-repudiation of the message. The secret key (α, β, SK) of our scheme used in HMAC is dynamic and encrypted by a hash function. Our scheme also adopts the temporary updated information in HMAC, so it is impossible for $\mathcal{A}$ to obtain these data. Therefore, this mechanism ensures that only the legitimate OBU_i or RSU_i can encrypt and decrypt the message with a dynamic secret key at each session. Therefore, our scheme provides non-repudiation of the message.

5) STOLEN VEHICLE ATTACK

It is possible for $\mathcal{A}$ to steal the vehicle and obtain the information stored in the memory of the OBU, which means that $\{PID_i^{old}, CN_i, \tau_i, PD, st^{old}, PSK^{old}, V\}$ can be stolen by $\mathcal{A}$. In our scheme, all of the stored information is encrypted in hash and XOR functions with the random number RN_i. Therefore, it is impossible for $\mathcal{A}$ to obtain information about ID_i, PW_i, and BIO_i according to the property of the hash function. However, $\mathcal{A}$ may try to guess RN_i with a negligible probability approximately equal to $\frac{1}{2^{24n+160+128}}$, where n represents ID_i, PW_i, ID_i, and ID_{SC} having n characters, and the length of the bio-hash output and random number are 160 and 128 bits, respectively. Therefore, our proposed scheme can withstand a stolen vehicle attack.

6) MUTUAL AUTHENTICATION AND IMPERSONATION ATTACK

Mutual authentication is the most important security property in wireless communications and $\mathcal{A}$ can impersonate any message sender through an impersonation attack. In our proposed scheme, we use the HMAC function to verify the legality of each sender, all of which functions consist of the temporary updated information and secret key which are encrypted by hash. This mechanism is safer than using a single encrypted parameter and constant information. Therefore, it is impossible for $\mathcal{A}$ to compute the verification message, and our scheme achieves mutual authentication and can withstand an impersonation attack.

7) REPLAY ATTACK

As the message is transmitted via a public channel, it is easy for $\mathcal{A}$ to launch a replay attack by resending of the intercepted message. In our scheme, the first step of every receiver is to check the freshness of the received message. If it is not fresh, then the receiver aborts any session open in any phases. Therefore, our scheme can resist replay attacks.

8) DECENTRALIZED AUTHENTICATION AND FAST-AUTHENTICATION

We assume the TA is compromised or that the channel between RSU and TA is damaged, then the centralized authentication is invalid and dangerous. In our scheme, the RSU can authenticate the OBU directly without the third trusted party. It reduces the cumbersome processes and risks associated with authentication. Furthermore, it can achieve a fast authentication for each of the OBUs. Therefore, our decentralized authentication scheme can achieve fast authentication and avoids the risks of a compromised TA or communication channel.

TABLE 2. Security comparison of the proposed scheme with other schemes.

Schemes	Mohit et al.	Zhou et al.	Liu et al.	Zhong et al.	Ours
Malicious authenticated vehicle attack	No	No	No	No	Yes
Anonymity	Yes	Yes	Yes	Yes	Yes
Tracking attack	No	Yes	Yes	No	Yes
Non-repudiation of message	No	No	No	Yes	Yes
Stolen vehicle attack	No	Yes	Yes	No	Yes
Mutual authentication	No	Yes	No	No	Yes
Reply attack	No	No	Yes	Yes	Yes
Offline guessing attack	No	Yes	Yes	No	Yes
Online guessing attack	Yes	Yes	Yes	Yes	Yes
Integrity of message	No	Yes	No	No	Yes
Privileged insider attack	No	Yes	Yes	No	Yes
Fast-authentication	No	Yes	No	No	Yes
V2V secret communication	No	Yes	Yes	Yes	Yes
Updated phase	Yes	Yes	Yes	Yes	Yes
Smart card revocation phase	No	No	No	No	Yes

9) OFFLINE GUESSING ATTACK

Offline guessing attacks are a major threat to any scheme based on passwords [39]. Using this method, $\mathcal{A}$ could hack into the OBU_i and obtain the information stored in its memory. In our scheme, the ID_i and PW_i are encrypted by the random number RN_i, which cannot be computed or guessed by $\mathcal{A}$, and which is analyzed in stolen smart card attack. Therefore, it is impossible for $\mathcal{A}$ to guess the ID_i and PW_i in an offline model. In addition, $\mathcal{A}$ may guess the biometric BIO_i from the stored information where BIO_i is hashed through a bio-hash function and stored in the encrypted form $(\sigma_i, \tau_i) = Gen(BIO_i)$, $RPW = h(RN_i \parallel \sigma_i \parallel PW_i \parallel ID_i)$. It is impossible for $\mathcal{A}$ to compute BIO_i in polynomial time according to the property of the hash function. However, $\mathcal{A}$ may attempt to guess BIO_i with the negligible probability of guessing approximately $\frac{1}{2^{24n+160+128}}$, where n represents ID_{SC}, ID_i, ID_v, and PW_i having n characters, and where the lengths of σ_i and RN_i are 160 bits and 128 bits, respectively. Therefore, our scheme can withstand offline guessing attacks.

10) ONLINE GUESSING ATTACK

In our scheme, the authentication phase negotiates the SK between OBU_i and RSU_i, and the V2V key agreement phase negotiates SK_{i-j} between OBU_i and OBU_j. It is impossible for $\mathcal{A}$ to compute the parameters of SK and SK_{i-j} owing to the properties of hash and symmetric encryption. However, if we assume that $\mathcal{A}$ attempts to guess SK and SK_{i-j}, then the probability of guessing these values is approximately equal to the negligible $\frac{1}{2^{128+128+160+160}}$ and $\frac{1}{2^{160+32}}$, respectively, where the lengths of the random numbers, timestamp and hash function are 128 bits, 32 bits, and 160 bits, respectively. Therefore, our proposed scheme can resist online guessing attacks.

11) INTEGRITY OF MESSAGE

The integrity, availability, and confidentiality of an information system are its most important properties [40]. Since a message may be lost during transmission, it is necessary to check the integrity of each transmitted message in any communication network [35]. In our scheme, we use the HMAC function to validate the integrity of the transmitted message, which is encrypted in HMAC using the secret key. If any bits are lost, then the output of the Ver function cannot be equal to 1, and the receivers may abort the session. Therefore, our scheme can check the integrity of the messages.

12) PRIVILEGED INSIDER ATTACK

If we assume $\mathcal{A}$ can obtain the information $\{A_i^{old}, PK_V^{old}, st^{old}, PSK^{old}, PID_i^{old}\}$, which are stored in the RSU, then according to the property of the hash, it is impossible to derive RN_i and d from A_i^{old} and PK_V^{old}, respectively, in polynomial time. However, $\mathcal{A}$ may use a guessing attack to obtain RN_i and d with negligible probabilities approximately equal to $\frac{1}{2^{128+128+160}}$ and $\frac{1}{2^{160+160+128}}$, respectively, where the length of the random number and hash function are 128 bits and 160 bits, respectively. Therefore, our scheme can withstand the privileged insider attack.

VI. COMPARISON WITH OTHER SCHEMES

We compare our proposed scheme in terms of security performance and overhead performance with the existing approaches from Zhou *et al.* [7], Mohit *et al.* [13], Liu *et al.* [14], and Zhong *et al.* [18].

A. SECURITY COMPARISON

In this section, we compare our scheme with others in terms of 12 security requirements and 3 functional phases, through a detailed and comprehensive analysis given in Table 2.

TABLE 3. The definition and execution time of computational operations.

Operation	Definition	Execution time (ms)
T_H	The hash function operation	0.0004
T_M	The HMAC generation and verification	0.0004
T_E	The symmetric encryption/decryption	0.1303
T_{EC}	The elliptic curve point multiplication	0.442
T_{BP}	The bilinear pairing operations	6.28
T_F	The fuzzy extractor operation	0.442
T_{BH}	The bio-hashing operation	0.442

We demonstrate that our proposed scheme provides the best security performance and most functionality for practical application. Yes/No represents whether the scheme can resist an attack or fulfill the corresponding security requirement, and the security properties are detailed below Table 2.

B. PERFORMANCE COMPARISON

With increasing speed and rapid changes in the network of AVs, the overhead performance of the authentication scheme is crucial. According to the network model of VSNs, the primary overhead is due to the computational and communication needs of the OBU_i and RSU_i.

1) THE BASE FOR COMPARISON

Compared with complicated computational operations, the overhead of some core functions required by the scheme cost far less and may be ignored, including the XOR, retrieving of the timestamp, generating a random number, and bitwise [41]. According to [7] and [42]–[45], the definition and execution time of related computational operations are shown in Table 3.

According to the advanced encryption standard proposed by the US Department of Commerce [46], the output of a hash and one prime factor is 160 bits, the length of the elliptic-curve point and bilinear pairing is 320 bits [47], the random number and HMAC is 128 bits, the ID_{SC}, ID_i, and ID_V are 160 bits, and the timestamp is 32 bits.

2) OVERHEAD COMPARISON WITH OTHER SCHEMES

For the overhead, we compare our proposed scheme with others in the aspects of the login, authentication, and V2V key agreement phases. We only compare the single authentication phase between the vehicle and RSU and the key agreement phase between two vehicles. The overheads of the login and authentication phases are compared in Table 4, the overhead of the V2V key agreement phase in Table 5, and the total overhead in Table 6. As Mohit *et al.* [13] do not include a V2V key agreement phase, their comparison in Table 5 is marked as N/A. The notations in these tables include Comp, the computation overhead, and Comm, the communication overhead. The data in each table are given to three decimal places.

TABLE 4. The overhead comparison of login and authentication phase.

Schemes	Comp		Comm (bits)		Total	
	OBU_i	RSU_i	OBU_i	RSU_i	Comp (ms)	Comm (bits)
Mohit et al.	$11T_H$	$9T_H$	928	768	0.008	1696
Zhou et al.	$12T_H$	$9T_H$	928	640	0.0084	1568
Liu et al.	$4T_H + 2T_{BP} + T_E$	$5T_H + 3T_{BP} + 3T_E$	1504	2304	31.92	3808
Zhong et al.	$7T_H + 3T_{EC}$	$16T_H + 5T_{EC}$	864	2976	3.55	3840
Ours	$12T_H + T_F + 2T_M + T_E$	$12T_H + 2T_M + T_E$	640	320	0.327	960

TABLE 5. The overhead comparison of V2V session key agreement phase.

Schemes	Comp		Comm (bits)		Total	
	OBU_i	OBU_j	OBU_i	OBU_j	Comp (ms)	Comm (bits)
Mohit et al.	N/A	N/A	N/A	N/A	N/A	N/A
Zhou et al.	$8T_H + 7T_{EC}$	$6T_H + 7T_{EC}$	800	640	3.1	1440
Liu et al.	$T_{BP} + 2T_H$	$T_{BP} + 2T_H$	1152	1152	18.84	2304
Zhong et al.	$2T_H + T_{EC}$	$T_H + T_{EC}$	192	192	0.885	384
Ours	$T_H + T_E$	$T_H + T_E$	224	224	0.261	448

As the VSNs is delay-sensitive networks, the delay time is a vital parameter for measuring the performance of scheme [48]. In V2V communication phase, the delay time of authentication scheme is mainly caused by verifying the signature and certificate of safety-related message [4], [19]. The performance evaluation of the schemes in terms of the execution time consumed to send traffic-related message by OBU is compared in Table 7 and shown in Fig.6. We only compare the worst case is that the OBU sends authentication message for each traffic-related messages [18]. As there are no V2V communication phase in Mohit *et al.*'s scheme, their scheme is not analyzed in this part.

From the tabulated security performance, overhead comparisons, and verification delay comparisons, we see that our proposed scheme is better than other schemes. Although the total computational overhead of our proposed scheme

TABLE 6. The total overhead comparison.

Schemes	Comp (ms)	Comm (bits)
Mohit et al.	0.008	1696
Zhou et al.	3.1	3008
Liu et al.	50.76	6112
Zhong et al.	4.435	4224
Ours	0.458	1344

TABLE 7. The comparison of verification delay

Schemes	Single traffic-related message	n traffic-related messages
Zhou et al.	$14T_H + 14T_{EC} \approx 6.19\ ms$	$14nT_H + 14nT_{EC} \approx 6.19n\ ms$
Liu et al.	$T_{BP} + 3T_H + 3T_{EC} \approx 7.62$ms	$nT_{BP} + 3nT_H + 3nT_{EC} \approx 7.62$n ms
Zhong et al.	$T_{EC} + 6T_H \approx 0.44$ms	$nT_{EC} + 6nT_H \approx 0.44$n ms
Ours	$T_H + T_E \approx 0.13$ms	$nT_H + nT_E \approx 0.13$n m

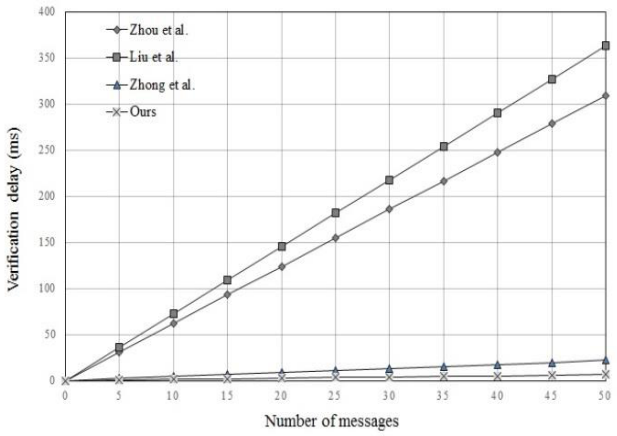

FIGURE 6. The comparison of verification delay.

is larger than Mohit *et al.*'s, our approach offers a greater number of applicable functions and is much safer. Therefore, our proposed scheme provides a better trade-off between security and efficiency.

VII. CONCLUSION AND FUTURE WORK

This paper has proposed a decentralized authentication scheme that uses continuously updated information for the V2R communication phase. Through validation and detailed analyses, our scheme can achieve fast authentication and is able to negotiate a secret and temporary SK for the V2R and V2V communication phases. Through the formal and informal security performance analysis, our scheme can withstand the related attacks including the tracing attack and the malicious authenticated vehicle attack. From the detailed overhead performance analysis, we find that our proposed scheme has a relatively small computation overhead, communication overhead, and delay time compared to other schemes. Therefore, we can draw the conclusion that our proposed scheme can resist various attacks and offers a better trade-off between security and efficiency compared to the existing schemes. In our future work, we will continue to research the development of adversary-related technologies incorporating batch authentication with a smaller overhead, as well as research more suitable V2R authentication schemes and V2V key agreement phases to reduce the operation and delay time of the RSU and OBU.

ACKNOWLEDGMENT

This research has no sponsors of any kind and the authors would like to thank their kind colleagues from the Laboratory of Information Security at Lanzhou University for their assistance with this paper. Finally, they sincerely thank the anonymous referees for their outstanding suggestions and constructive feedback.

REFERENCES

[1] T. Toroyan, "Global status report on road safety: Time for action," *Injury Prevention*, vol. 15, p. 286, 2009. [Online]. Available: https://injuryprevention.bmj.com/content/15/4/286, doi: 10.1136/ip.2009.023697.

[2] Z. Ning, F. Xia, N. Ullah, X. J. Kong, and X. P. Hu, "Vehicular social networks: Enabling smart mobility," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 16–55, May 2017.

[3] Z. Ning *et al.*, "A cooperative quality-aware service access system for social Internet of vehicles," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2506–2517, Aug. 2018.

[4] K. Zaidi and M. Rajarajan, "Vehicular Internet: Security & privacy challenges and opportunities," *Future Internet*, vol. 7, no. 3, pp. 257–275, 2015.

[5] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.

[6] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Veh. Commun.*, vol. 9, pp. 19–30, Jul. 2017.

[7] 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.

[8] M.-C. Chuang and J.-F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," in *Proc. Int. Conf. Consum. Electron., Commun. Netw.*, Apr. 2011, pp. 1758–1761.

[9] X. Wang *et al.*, "A city-wide real-time traffic management system: Enabling crowdsensing in social Internet of vehicles," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 19–25, Sep. 2018. [Online]. Available:https://ieeexplore.ieee.org/document/8466350, doi: 10.1109/MWC.2018.1700441.

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

[11] P. Kumar, S. Kumari, V. Sharma, X. Li, A. K. Sangaiah, and S. H. Islam, "Secure CLS and CL-AS schemes designed for VANETs," *J. Supercomput.*, vol. 74, pp. 1–23, Mar. 2018.

[12] 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, pp. 4255–4271, Nov. 2016.

[13] P. Mohit, R. Amin, and G. P. Biswas, "Design of authentication protocol for wireless sensor network-based smart vehicular system," *Veh. Commun.*, vol. 9, pp. 64–71, Jul. 2017.

[14] 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.
[15] 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.
[16] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy, "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks," *Cluster Comput.*, vol. 20, no. 3, pp. 2439–2450, 2017.
[17] J. Li *et al.*, "EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *Veh. Commun.*, vol. 13, pp. 104–113, Jul. 2018.
[18] H. Zhong, B. Huang, J. Cui, Y. Xu, and L. Liu, "Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks," *IEEE Access*, vol. 6, pp. 2241–2250, 2018.
[19] C. Li, X. Zhang, H. Wang, and D. Li, "An enhanced secure identity-based certificateless public key authentication scheme for vehicular sensor networks," *Sensors*, vol. 18, no. 1, p. 194, 2018.
[20] C.-L. Chen, M.-L. Chiang, C.-C. Peng, C.-H. Chang, and Q.-R. Sui, "A secure mutual authentication scheme with non-repudiation for vehicular ad hoc networks," *Int. J. Commun. Syst.*, vol. 30, no. 6, p. e3081, 2017.
[21] X. Wang, S. Li, S. Zhao, Z. Xia, and L. Bai, "A vehicular ad hoc network privacy protection scheme without a trusted third party," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 12, p. 155014771774369, 2017.
[22] S. Wang and N. Yao, "LIAP: A local identity-based anonymous message authentication protocol in VANETs," *Comput. Commun.*, vol. 112, pp. 154–164, Nov. 2017.
[23] X. Tian and S. Qiang, "Research of an authentication scheme based on the proxy blind signature scheme for the vehicular ad-hoc networks," *Bull. Sci. Technol.*, vol. 28, no. 10, pp. 170–173, 2012.
[24] X. Wang, S. Li, S. Zhao, and Z. Xia, "A VANET privacy protection scheme based on fair blind signature and secret sharing algorithm," *Automatika*, vol. 58, no. 3, pp. 287–294, 2017. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/00051144.2018.1426294, doi: 10.1080/00051144.2018.1426294.
[25] N. Kumar, R. Iqbal, S. Misra, and J. J. P. C. Rodrigues, "An intelligent approach for building a secure decentralized public key infrastructure in VANET," *J. Comput. Syst. Sci.*, vol. 81, no. 6, pp. 1042–1058, 2015.
[26] Z. Ning, P. Dong, X. Kong, and F. Xia, "A cooperative partial computation offloading scheme for mobile edge computing enabled Internet of Things," *IEEE Internet Things J.*, to be published. [Online]. Available: https://ieeexplore.ieee.org/document/8454442, doi: 10.1109/JIOT.2018.2868616.
[27] X. Wang *et al.*, "A privacy-preserving message forwarding framework for opportunistic cloud of things," *IEEE Internet Things J.*, to be published. [Online]. Available: https://ieeexplore.ieee.org/document/8432066, doi: 10.1109/JIOT.2018.2864782.
[28] Z. Ning, X. Kong, F. Xia, W. Hou, and X. Wang, "Green and sustainable cloud of things: Enabling collaborative edge computing," *IEEE Commun. Mag.*, to be published. [Online]. Available: https://www.researchgate.net/publication/325742943_Green_and_Sustainable_Cloud_of_Things_Enabling_Collaborative_Edge_Computing, doi: 10.1109/MCOM.2018.1700895.
[29] Z. Ning, J. Huang, and X. Wang, "Vehicular fog computing: Enabling real-time traffic management for smart cities," *IEEE Wireless Commun.*, to be published. [Online]. Available: https://www.researchgate.net/publication/325742707_Vehicular_Fog_Computing_Enabling_Real-time_Traffic_Management_for_Smart_Cities, doi: 10.1109/MWC.2018.1700441.
[30] Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: Applications and related technical issues," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 3, pp. 74–88, 3rd Quart., 2008.
[31] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Netw.*, vol. 32, pp. 17–31, Sep. 2015.
[32] F. Wen, "A robust uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care," *J. Med. Syst.*, vol. 37, no. 6, p. 9980, 2013.
[33] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.
[34] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 53–57, Jun. 2004.
[35] K. K. R. Choo, "On the security analysis of Lee, Hwang & Lee (2004) and Song & Kim (2000) key exchange/agreement protocols," *Informatica*, vol. 17, no. 4, pp. 467–480, 2005.
[36] V. V. Vinod and S. Ghose, "Point matching using asymmetric neural networks," *Pattern Recognit.*, vol. 26, no. 8, pp. 1207–1214, 1993.
[37] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," in *Proc. 12th ACM Symp. Oper. Syst. Princ.*, 1989, pp. 1–13.
[38] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, and J. Cuellar, "The AVISPA tool for the automated validation of Internet security protocols and applications," in *Computer Aided Verification*. Berlin, Germany: Springer, 2005.
[39] J. Nam, K.-K. R. Choo, J. Paik, and D. Won, "Cryptanalysis of server-aided password-based authenticated key exchange protocols," *Int. J. Secur. Appl.*, vol. 7, no. 2, pp. 47–58, 2013.
[40] P. Singh, P. K. Sharma, and T. K. Aggarwal, "Cryptography and network security principles and practices," *Int. J. Eng. Comput. Sci.*, vol. 1, no. 1, pp. 121–136, 2012.
[41] C.-C. Lee, C.-T. Chen, P.-H. Wu, and T.-Y. Chen, "Three-factor control protocol based on elliptic curve cryptosystem for universal serial bus mass storage devices," *IET Comput. Digit. Techn.*, vol. 7, no. 1, pp. 48–56, Jan. 2013.
[42] J. Nam, K.-K. R. Choo, S. Han, M. Kim, J. Paik, and D. Won, "Efficient and anonymous two-factor user authentication in wireless sensor networks: Achieving user anonymity with lightweight sensor computation," *PLoS ONE*, vol. 10, no. 4, p. e0116709, 2015.
[43] J. Jung, J. Moon, D. Lee, and D. Won, "Efficient and security enhanced anonymous authentication with key agreement scheme in wireless sensor networks," *Sensors*, vol. 17, no. 3, p. 644, 2017.
[44] A. K. Das, A. K. Sutrala, V. Odelu, and A. Goswami, "A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks," *Wireless Pers. Commun.*, vol. 94, pp. 1899–1933, Jun. 2017.
[45] F. Wu, L. Xu, S. Kumari, and X. Li, "A new and secure authentication scheme for wireless sensor networks with formal proof," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 1, pp. 16–30, 2017.
[46] U.S. Department of Commerce, "Advanced encryption standard," in *Proc. Nat. Comput. Conf.*, 1997, pp. 83–87.
[47] *Secure Hash Standard (SHS)*, Federal Information Processing Standards Publication 180-4, U.S. Department of Commerce, 2012.
[48] Z. Ning, L. Liu, F. Xia, B. Jedari, I. Lee, and W. Zhang, "CAIS: A copy adjustable incentive scheme in community-based socially aware networking," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3406–3419, Apr. 2017.

XIN LIU received the B.S. degree in communication engineering and the M.Sc. degree in computer application technology from Lanzhou University, Lanzhou, China, in 2011 and 2014, respectively, where he is currently pursuing the Ph.D. degree with the School of Information Science and Engineering. His research interests include cryptography, wireless sensor network security, remote user authentication, and protocol design.

RUISHENG ZHANG received the B.S. degree from the Department of Mathematics, Lanzhou University, in 1983, and the M.A. and Ph.D. degrees from the Department of Chemistry, Lanzhou University, in 1990 and 1996, respectively. He is currently a Professor and a Ph.D. Supervisor with the School of Information Science and Engineering, Lanzhou University. He is a Key Member of the Virtual Chemical Lab, Computer Network Information Center, Chinese Academy of Sciences. The main research fields are high performance and grid computing, service computing, and information security. He is a member of The Institution of Engineering and Technology and a Senior Member of the China Computer Federation (CCF) and the Technical Committee on Service Computing of CCF.