An Efficient and Provably-Secure Authenticated Key Agreement Protocol for Fog-Based Vehicular Ad-Hoc Networks

Mimi Ma, Debiao He, Huaqun Wang, Neeraj Kumar, Kim-Kwang Raymond Choo

***Abstract*—Recently, the maturity of cloud computing, the internet of things (IoT) technology and intelligent transportation system (ITS) has promoted the rapid development of vehicular ad-hoc networks (VANETs). To keep pace with real-world demands (i.e., mobility, low latency, etc.) in a practical VANETs deployment, there have been attempts to integrate fog computing into the VANETs. To facilitate secure interaction in a fog-based VANETs, we design a new authenticated key agreement (AKA) protocol without bilinear pairing. This protocol achieves mutual authentication, generates a securely agreed session key for secret communication, and supports privacy protection. We also give a strict formal security proof and demonstrate how the proposed protocol meets the security requirements in the fog-based VANETs. We then evaluate the efficiency of the proposed protocol, and it shows the practicality of the protocol.**

***Index Terms*—Security, fog computing, vehicular ad-hoc networks, VANETs, fog-based VANETs, authenticated key agreement.**

I. Introduction

As the third wave of the world's information industry after the computer and the internet, the IoT technology will be the next significant productivity driver for promoting the world's development. More specifically, it can achieve remote monitoring, automatic alarm, diagnosis and many other functional properties, using various sensing technologies (i.e., RFID, sensors) and communication modes (i.e., wired or wireless) to connect special objects to the network. With the above features, it has been applied in a wide range of fields, such as environment protection, smart home, intelligent healthcare, intelligent transportation system (ITS) and so on. In particular, with the emergency of IoT technology, ITS has arouse extensive attention in academia and industry [1].

ITS is a large-scale, real-time and effective traffic control system. In ITS, an intelligent transportation center (ITC) is mainly responsible for collecting and decision-making traffic information, and returning the decision-making results to roadside related facilities, which can effectively ease traffic congestion, improve transport efficiency, reduce traffic accidents, and minimize energy consumption and environmental pollution. However, there are still a number of urgent problems to solve [2]. For example, as more vehicles (e.g. driverless vehicles) and related devices join the ITS, how to deal with the corresponding increase in computational and processing demands, particularly in complex and constant changing traffic situations, is extremely challenging.

One of the potential solutions is the distributed traffic control system (DTCS), an extension of VANETs in order to support communication and information processing capabilities and efficient allocation of road resources [3], [4]. VANETs can be considered as a special type of mobile network, but having vehicles (instead of mobile devices) as nodes. Vehicles are equipped with on-board units (OBUs) to facilitate vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications.

In V2V communication, each vehicle periodically broadcasts messages (i.e., the vehicle's speed and position) to surrounding vehicles. This allows the vehicle or other vehicles in the vicinity to adjust the route in real time if necessary. In addition, a vehicle can also send a specific message to a specific target vehicle, and only the latter can correctly parse the message after receiving the message. In V2I communication, a vehicle can request for some services from the nearby roadside units (RSUs). The RSUs act as a transfer station and will forward the messages to an authentication center or a service provider.

Both V2V and V2I communications are mainly conducted via wireless technology, i.e., dedicated short-range communication (DSRC). DSRC allows one to recognize and communicate with moving targets at high speed within a small physical range, and transmit data information (e.g., voice, image, etc.) in real time. Hence, vehicles and the supporting infrastructures can connect organically, for example to improve

The work of as supported by the National Natural Science Foundation of China under Grant No. 61572379, Grant No. 61572370, and Grant No. 61872192, the High-level talent Fund Project of Henan University of Technology under Grant No. 31401164, the Natural Science Foundation of Jiangsu Province under Grant No. BK20181394, Qing Lan Project of Jiangsu Province, 1311 Talent Plan Foundation of NUPT.

M. Ma is with the College of Information Science and Engineering, Henan University of Technology, Zhengzhou, China
E-mail: mamimi421@126.com

D. He (*Corresponding author*) is with the School of Cyber Science and Engineering, Wuhan University, Wuhan, China
E-mail: hedebiao@163.com

H. Wang is with the Jiangsu Key Laboratory of Big Data Security and Intelligent Processing, School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, China
E-mail: wanghuaqun@aliyun.com

N. Kumar is with the Department of Computer Science and Engineering, Thapar University, Patiala, India
E-mail: nehra04@yahoo.co.in

K.-K. R. Choo is with the Department of Information Systems and Cyber Security and the Department of Electrical and Computer Engineering, The University of Texas at San Antonio, San Antonio, TX 78249, USA
Email: raymond.choo@fulbrightmail.org

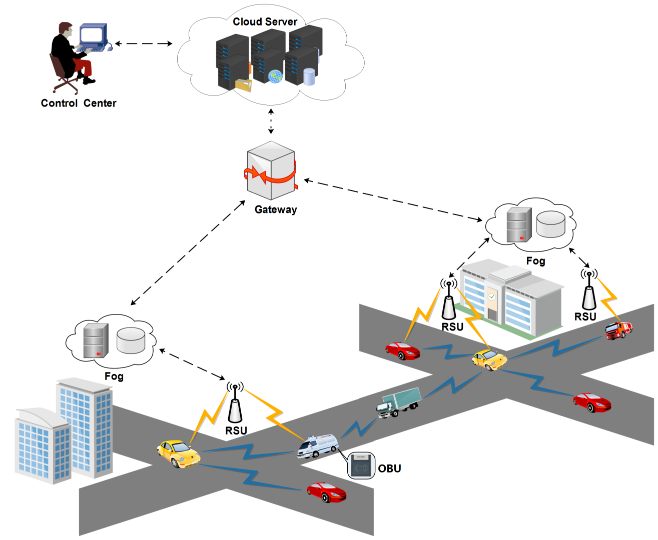

Fig. 1. A typical fog-based VANETs structure

traffic situation (e.g., reducing traffic jam and accident rate) and provide various services (e.g., early warning of driving safety, assistance driving, traffic information release, and vehicle entertainment).

However, with the rapid increase in the number of vehicles and the changing demand for services in recent years, the amount of data generated and needed to be processed has also increased [5]–[7]. Using cloud computing to address such challenges has brought additional issues. For example, as the cloud server is far from the vehicle terminals, there must be issues related to network bandwidth, latency and so on. Consequently, it is a challenging work to handle emergencies on the road in real-time [8].

Recently, there have been efforts to extend cloud computing to the edge of the network, for example deploying fog nodes to the network edge [9]. In other words, computational capabilities (i.e., data storage and computing) are pushed to devices located on the edge of network, which aligns with the "decentralization" feature of the internet. This allows some services to be decentralized from the cloud to the fog devices [10], [11], and hence reduces data transmission delay, bandwidth consumption, computational costs and so on [12]. Fig. 1 shows a typical fog-based VANETs structure.

Furthermore, in the context of VANETs, fog computing can potentially facilitate the following:

1) timely detection of dangerous driving behavior, providing early warning and imposing appropriate punishment, if needed (e.g., by deploying sensors on vehicles and both sides of the road) [13];
2) real-time traffic control, for example by changing the timing of the traffic lights when there is no approaching vehicle, from the obtained information such as sensing speed and road conditions;
3) real-time reminders, for example to warn drivers to slow down in emergency situations (e.g., approaching ambulances or police vehicles) by controlling traffic lights based on the monitoring data from sensors.

However, there are underpinning security risks that need to be addressed [14], [15]. For example, how do we efficiently secure the fog devices deployed on the edge of the network, ensure the stability and reliability of the transmitted data, and detect malicious behavior (e.g., tampering or deleting of data-in-transit). To improve data confidentiality and privacy, users (vehicles) can pre-encrypt their data prior to transmission. However, sharing session keys in advance between entities is expensive, in terms of computation and communication costs, particularly in applications where mobility is essential (e.g., VANETs).

Authenticated key agreement (AKA) protocols, such as those presented in [16], [17], can achieve mutual authentication between entities and generate a common session key. However, only a few of the existing AKA protocols can be applied to the fog-based environments. Recently, Jia *et al.* [18] used bilinear pairings to design an AKA protocol for fog-driven healthcare system, and their protocol was proven secure in random oracle model. However, bilinear pairings are computational expensive. Moreover, in order to construct AKA protocols that can be deployed in real-time and high-speed moving application environments such as VANETs, we need to minimize key negotiation time as much as possible. Hence, in this paper, we extend Jia *et al.*'s solution to support fog-based VANETs by removing the need for bilinear pairings.

Specifically, in this paper we design an efficient three-party AKA protocol without using bilinear pairings. The protocol achieves both mutual authentication and key establishment/agreement. The protocol is then proven secure in the random oracle model, and is shown to fulfill the security requirements of fog-based VANETs. In the next two sections, we review the existing literatures and relevant background materials. In section IV, we present our proposed protocol. In sections V and VI, we present the security and efficiency analysis of the new protocol, respectively. Section VII summarizes our work.

II. Related Work

To enhance data privacy and security in VANETs, a conditional privacy preservation authentication (CPPA) protocol is constructed by Raya *et al.* [19]. In their protocol, the OBUs configured in the vehicle requires many private keys and corresponding anonymous certificates to be loaded in advance so as to protects vehicles' real identities. During driving, the vehicle will randomly choose a private key and a certificate to broadcast messages. And a certificate authority (CA) stores the corresponding relationship of the vehicle and the anonymous certificate. In order to achieve anonymity more effectively, the vehicle will revoke the original anonymous certificate after a period of driving, and then randomly select a new anonymous certificate to broadcast messages. However, it requires huge storage space to save each vehicle's anonymous certificate and costs high traceability overheads.

To address these issues, Lu *et al.* [20] designed a new CPPA protocol for VANETs. In [20], each vehicle can obtain a temporary anonymous certificate from RSUs instead of applying for an anonymous certificate from CA. Later, Sun *et al.* [21] designed an efficient RSUs deployment protocol, which allows vehicle nodes to update certificates in a short time without holding a large certificate revocation list. Freudiger *et al.* [22] presented a new CPPA protocol by combining the technologies of mix-zones and anonymous certificates. However, in [22], RSUs or vehicles have to store many certificates.

Zhang *et al.* [23] exploited message authentication code to construct a novel authentication protocol that can be applied to VANETs, in which the session key between a vehicle and a RSUs was generated using a key agreement protocol. To enhance the privacy and confidentiality, a different private/public key pair and the binding certificate should be selected when the vehicle communicates with RSUs each time. But the key and certificate management is cumbersome.

Zhang *et al.* [24] designed an identity-based CPPA protocol for VANETs to address the above certificate management issue. Their proposal relies on tamper-proof devices loaded in vehicles to store the private keys that generate pseudo identities according to the method (i.e., using an identity-based cryptosystem) introduced in [25]. In addition, a batch signature verification method is introduced in the communication between vehicles and RSUs to lessen the cost of verification. Zhang *et al.* [26] provided a new CPPA protocol to avoid using expensive tamper-proof devices. Later, Lee *et al.* [27] found that protocol [24] can neither resist replay attack nor satisfy non-repudiation of a signature, and they used bilinear pairings to design a more efficient authentication protocol. Unfortunately, Bayat *et al.* [28] stated protocol [27] is subjected to an impersonation attack (i.e., an attacker can impersonate the other vehicles to produce a valid signature). To solve the weaknesses that exist in [27], Bayat *et al.* [28] designed a new authentication protocol.

Liu *et al.* [29] used distributed computing to construct a proxy based authentication (PBA) protocol for VANETs. In [29], the proxy vehicle could use a verification function to authenticate multiple messages simultaneously, thereby reducing the computational costs of RSUs. In the same year, He *et al.* [30] designed a CPPA protocol without using bilinear pairings. And recently, Lo *et al.* [31] introduced a new identity-based signature mechanism, and constructed an efficient CPPA protocol free from bilinear pairings based on the above signature. Asaar *et al.* [32] presented that protocol [29] suffers from the impersonation and modification attacks. To address the shortcomings of protocol [29], Asaar *et al.* designed a new identity-based PBA protocol in [32]. Furthermore, they show their protocol is secure against existential forgery on adaptively chosen identity and message attacks under the elliptic curve discrete logarithm (ECDL) problem assumption in random oracle model. Later, Li *et al.* [33] proposed anonymous CPPA protocol to protect the privacy of VANETs.

Büttner *et al.* [34] combined a ring signature and an elliptic curve integrated encryption mechanism to construct an anonymous AKA protocol for the security of message transmission between vehicles in VANETs. Dang *et al.* [35] designed an identity-based AKA protocol without bilinear pairings for VANETs. In addition, their protocol is proved to be secure in the extended Canetti-Krawczyk model [36] under Gap Diffie-Hellman assumption.

Nowadays, many authentication solutions and AKA protocols have been constructed for VANETs. However, most of the proposed protocols cannot be directly applied to the fog-based structure. Recently, Jia *et al.* [18] proposed an AKA protocol with bilinear pairings for healthcare system under fog computing environment. However, a bilinear pairing operation is expensive in basic operations. To improve the efficiency, a new AKA protocol to avoid the use of bilinear pairings was presented in this paper.

III. Background

A. Complexity Assumptions

We assume that $\mathbb{G}$ is a cyclic additive group with q-order, where q is a large prime number. Let $P \in \mathbb{G}$ be a generator.

ECDL assumption: i.e., the problem of elliptic curve discrete logarithm. That is, given two points $P \in \mathbb{G}$ and $xP \in \mathbb{G}$, the advantage of calculating $x \in \mathbb{Z}_q^*$ in probability polynomial time is negligible.

ECCDH assumption: i.e., the problem of elliptic curve computational Diffie-Hellman. That is, given three points $P \in \mathbb{G}$, $xP \in \mathbb{G}$ and $yP \in \mathbb{G}$, the advantage of calculating xyP in probability polynomial time is negligible, where x and y are two unknown numbers in $\mathbb{Z}_q^*$.

ECDDH assumption: i.e., the problem of elliptic curve decisional Diffie-Hellman. That is, given four points P, $X = xP$, $Y = yP$ and $Z = zP$ in group $\mathbb{G}$ (x, y, $z \in \mathbb{Z}_q^*$ are unknown numbers), it's difficult to decide $Z \overset{?}{=} xyP$.

B. System Model

The system model of the proposed protocol for fog-based VANETs are presented in Fig. 2. There exist the following participants in the proposed protocol, i.e., a vehicle user (U_i), a fog node (FN_j), a RSU and a cloud server (CS).

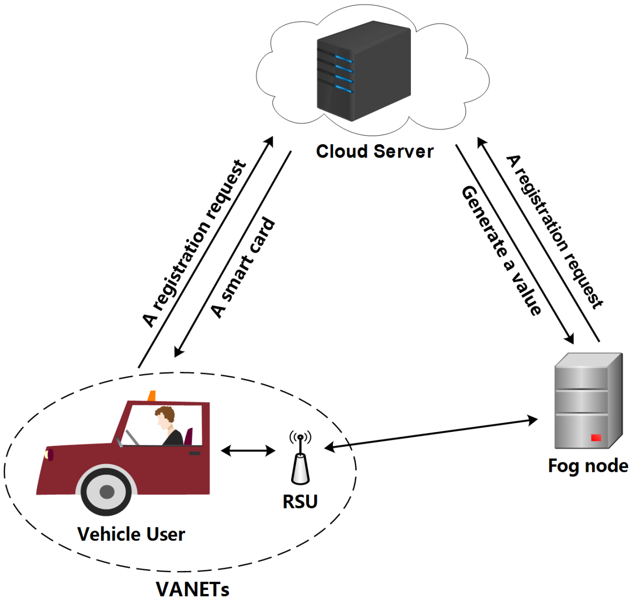

Fig. 2. The system model for fog-based VANETs

- U_i**:** It represents the i-th vehicle user. U_i controls the vehicle which is equipped with an OBU and connects to

FN_j via the nearby RSU. In addition, U_i should request a smart-card from CS using his/her identity. U_i can only pass the system authentication by entering the correct password and smart-card.

- FN_j**:** It is considered an untrustworthy participant and has certain computing and storage capacity. FN_j is responsible for providing authentication messages between CS and U_i. Finally, a common session key is negotiated between FN_j , CS and U_i.
- RSU**:** It is a wireless communication equipment, which is deployed on roadside infrastructure and only plays a gateway role in VANETs, mainly responsible for broadcasting and relaying.
- CS**:** It is a trusted cloud service provider which is in charge of producing system public parameters and the master private key s. Besides, CS provides the corresponding registration service for U_i and FN_j according to their registration request. For subsequent authentication, CS should store the verifiers which is derived from U_i's (or FN_j's) identity and the master key s.

C. Security Requirements

Privacy protection is crucial in fog-based VANETs. Thus, an AKA protocol for VANETs under fog computing environment should satisfy the following security requirements [37]–[41].

- **Mutual authentication:** In order to guarantee the validity of all participants, the AKA protocol needs to support mutual authentication.
- **Session key agreement:** In order to protect the confidentiality of information transmitted in the future interaction process, the AKA protocol needs support to generate a common session key among participants for encrypting messages.
- **User anonymity:** To protect the vehicle users' privacy, the three-party AKA protocol must have the user anonymity and un-traceability, in other words, even if an attacker intercepts the messages in process of the message transmission, the user's real identity cannot be extracted and the behavior of the user cannot be traced.
- **Un-traceability:** Even if an adversary intercepts the messages in the protocol transmission, it cannot track the user's behavior.
- **Perfect forward secrecy:** For protecting the privacy of messages transferred in previous interaction, an AKA protocol must offer perfect forward secrecy, namely, the session key that is established in previous session should still safe even if an attacker gets participants' long-term private keys.
- **Resistance of off-line dictionary attack:** An adversary is unable to guess and calculate the password of legitimate users using the information that it has obtained, including the messages of interaction, the data of smart-card, and the information stored on the server.
- **Resistance of stolen verifier attack:** When the contents of verifier table on cloud server are stolen, the attacker is incapable of deducing users' passwords from the verifier table contents.
- **Resistance of known session key attack:** Under the circumstance of knowing the session key generated in a given protocols, the adversary cannot calculate another secure session key.
- **Resistance of man-in-the-middle attack:** An attacker cannot pretend to be a legitimate user to cheat cloud server, nor can he impersonate the server to deceive legitimate users.
- **Resistance of replay attack:** The adversary cannot launch an attack on the protocol to replay the old messages.

IV. The Proposed AKA Protocol

We describe our new three-party AKA protocol for fog-based VANETs without bilinear pairings in this section. Five phases are included in our protocol, and the specific description is as follows.

A. Setup Phase

Take the security parameter k as input, the cloud server (CS) is implemented as follows to generate system parameters.

1) CS chooses a q-order additive group $\mathbb{G}$ with a generator P.
2) CS selects $s \in \mathbb{Z}_q^*$ randomly, and calculates $P_{pub} = sP$.
3) CS chooses six cryptographic hash function $h_i(i = 1, 2, 3, 4, 5, 6)$, where $h_1 : \{0,1\}^* \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $h_2 : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{Z}_q^*$, $h_3 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G} \times \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{Z}_q^*$, $h_4 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G} \times \mathbb{G} \times \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{Z}_q^*$, $h_5 : \mathbb{G} \times \mathbb{G} \times \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{Z}_q^*$, $h_6 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G} \times \mathbb{G} \times \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{Z}_q^*$, CS keeps s secretly, and publishes system parameters $prms = \{k, q, P, \mathbb{G}, P_{pub}, h_i\}$.

B. Vehicle User Registration Phase

The vehicle user U_i registers with CS to get a private key. Fig. 3 presents the interaction between U_i and CS.

1) U_i sends its identity ID_{U_i} to CS.
2) Upon receiving ID_{U_i}, CS calculates $D_{ID_i} = h_1(s, ID_{U_i})P$, and stores $\{ID_{U_i}, D_{ID_i}\}$ on a smart-card. Finally, CS returns the smart-card to U_i.

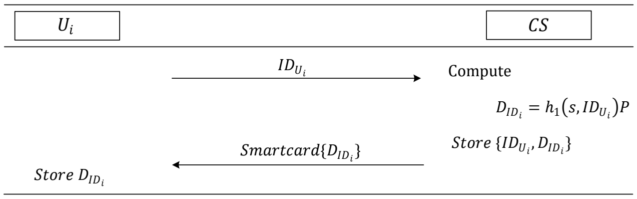

Fig. 3. The vehicle user registration phase

C. Fog Node Registration Phase

The fog node FN_j registers with CS to obtain a private key. Fig. 4 indicates the interaction between FN_j and CS.

1) FN_j transmits its identity ID_{FN_j} to CS.
2) CS calculates $D_{ID_j} = h_1(s, ID_{FN_j})P$, and returns D_{ID_j} to CS via a secure channel.
3) FN_j stores D_{ID_j} secretly and finishes the registration.

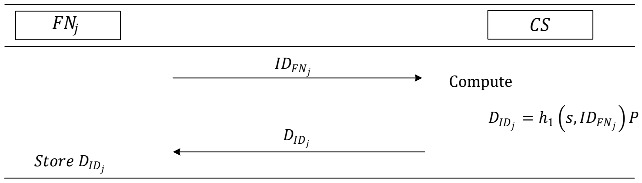

Fig. 4. The fog node registration

D. Mutual Authentication & Key Agreement Phase

The vehicle user U_i, the fog node FN_j and the cloud server CS perform the following operations separately to realize mutual authentication, and finally generate a common session key. Fig. 5 shows the interaction between them.

1) U_i selects a random number $r_1 \in \mathbb{Z}_q^*$. Let T_{U_i} denote the current timestamp. U_i calculates $R_1 = r_1 P$, $\bar{R}_1 = r_1 P_{pub}$, $AID_{U_i} = ID_{U_i} \oplus h_2(R_1, \bar{R}_1)$, $\alpha = h_3(ID_{U_i}, T_{U_i}, R_1, \bar{R}_1, D_{ID_i})$, and sends $\{AID_{U_i}, T_{U_i}, R_1, \alpha\}$ to FN_j.
2) FN_j checks the freshness of T_{U_i}, then selects $r_2 \in \mathbb{Z}_q^*$ randomly. Let T_{FN_j} denote the current timestamp. FN_j computes $R_2 = r_2 P$, $\hat{R}_2 = r_2 R_1$, $\bar{R}_2 = r_2 P_{pub}$, $AID_{FN_j} = ID_{FN_j} \oplus h_2(R_2, \bar{R}_2)$, and $\beta = h_4(AID_{U_i}, ID_{FN_j}, T_{U_i}, T_{FN_j}, R_1, R_2, \hat{R}_2, \bar{R}_2, D_{ID_j})$. At last, FN_j sends the messages $\{AID_{U_i}, AID_{FN_j}, T_{U_i}, T_{FN_j}, R_1, R_2, \hat{R}_2, \alpha, \beta\}$ to CS.
3) CS checks the validity of T_{U_i} and T_{FN_j}. Then CS calculates $\bar{R}'_1 = sR_1$, $\bar{R}'_2 = sR_2$, $ID'_{U_i} = AID_{U_i} \oplus h_2(R_1, \bar{R}'_1)$, $ID'_{FN_j} = AID_{FN_j} \oplus h_2(R_2, \bar{R}'_2)$, $D'_{ID_i} = h_1(s, ID'_{U_i})P$, $D'_{ID_j} = h_1(s, ID'_{FN_j})P$, $\alpha' = h_3(ID'_{U_i}, T_{U_i}, R_1, \bar{R}'_1, D'_{ID_i})$, $\beta' = h_4(AID_{U_i}, ID'_{FN_j}, T_{U_i}, T_{FN_j}, R_1, R_2, \hat{R}_2, \bar{R}'_2, D'_{ID_j})$. CS checks if both of $\alpha' = \alpha$ and $\beta' = \beta$ are true. If one of the two equations is incorrect, CS rejects the request. Otherwise, CS selects $r_3 \in \mathbb{Z}_q^*$ randomly and calculates $R_3 = r_3 P$, $\hat{R}_3 = r_3 R_1$, $\hat{R}'_3 = r_3 R_2$, $K_{CS} = r_3 \hat{R}_2$, $SK_{CS} = h_5(K_{CS}, R_1, R_2, R_3)$, $\gamma = h_6(D'_{ID_j}, T_{CS}, R_1, R_2, R_3, \hat{R}_3)$, $\bar{\gamma} = h_6(D'_{ID_i}, T_{CS}, R_1, R_2, R_3, \hat{R}'_3)$, where T_{CS} denotes the current timestamp. At last, CS sends $\{R_3, \hat{R}_3, \hat{R}'_3, T_{CS}, \gamma, \bar{\gamma}\}$ to FN_j.
4) FN_j checks the freshness of T_{CS}, and checks whether $\gamma = h_6(D_{ID_j}, T_{CS}, R_1, R_2, R_3, \hat{R}_3)$ holds. If not, FN_j aborts the request. Otherwise, FN_j calculates $K_{FN_j} = r_2 \hat{R}_3$,and $SK_{FN_j} = h_5(K_{FN_j}, R_1, R_2, R_3)$. At last, FN_j sends $\{R_2, R_3, \hat{R}'_3, T_{CS}, \bar{\gamma}\}$ to U_i
5) U_i checks the freshness of T_{CS} and verifies whether the equation $\bar{\gamma} = h_6(D_{ID_i}, T_{CS}, R_1, R_2, R_3, \hat{R}'_3)$ is true. If not, U_i terminates the session. Otherwise, U_i calculates $K_{U_i} = r_1 \hat{R}'_3$ and $SK_{U_i} = h_5(K_{U_i}, R_1, R_2, R_3)$.

Since $r_1 \hat{R}'_3 = r_2 \hat{R}_3 = r_3 \hat{R}_2 = r_1 r_2 r_3 P$, then we have $K_{U_i} = K_{FN_j} = K_{CS}$, it follows that $SK_{U_i} = SK_{FN_j} = SK_{CS}$. Hence, this verifies the correctness of our proposed protocol.

V. Security Analysis

In this section, firstly, a security model for our protocol is described. And then, our protocol is proved provably secure under above security model. Finally, our protocol is shown to meet the security requirements that presented in section III.

A. Security Model

Next, we use a series of games between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ to define the security model of our proposed protocol on the basis of Bellare *et al.*'s work [42]. Suppose the i-th instance of participant $\Lambda \in \{U, FN, CS\}$ is denoted by Π^i_Λ, and let Σ be the protocol. In these games, $\mathcal{A}$ can ask various oracle queries, and $\mathcal{C}$ responds as below.

- $Send(\Pi^i_\Lambda, m)$: If $\mathcal{A}$ asks the query with message m, then $\mathcal{C}$ runs the protocol according to specific steps and outputs the results.
- $Reveal(\Pi^i_\Lambda)$: Upon receiving $\mathcal{A}$'s query, if Π^i_Λ is accepted, then $\mathcal{C}$ outputs the session key. Otherwise, $\mathcal{C}$ returns $\perp$.
- $Corrupt(ID_{U_i})$: This query simulates forward security. If $\mathcal{A}$ asks the query with U_i's identity ID_{U_i}, $\mathcal{C}$ returns U_i's private key.
- $Execute(\Pi^i_U, \Pi^j_{FN}, \Pi^k_{CS})$: This query simulates the execution of the adversary $\mathcal{A}$ passive eavesdropping protocol. $\mathcal{C}$ outputs all messages of the instances Π^i_U, Π^j_{FN} and Π^k_{CS} that are transferred during the execution of the protocol.
- $Test(\Pi^i_\Lambda)$: If the adversary $\mathcal{A}$ asks the query, $\mathcal{C}$ selects a $b \in \{0, 1\}$ randomly. If $b = 1$, then $\mathcal{A}$ gets the session key involved in Π^i_Λ. Otherwise, $\mathcal{C}$ randomly selects a number that has the same length as the session key, and sends the number to $\mathcal{A}$.

***Definition** 1 (Partnership):* If the instances Π^i_Λ and $\Pi^i_{\bar{\Lambda}}$ has the properties listed below, then we say Π^i_Λ and $\Pi^i_{\bar{\Lambda}}$ are *partner*:

1) Π^i_Λ can exchange information with $\Pi^i_{\bar{\Lambda}}$ directly;
2) Π^i_Λ and $\Pi^i_{\bar{\Lambda}}$ share the same session key SK;
3) There is no instance to accept SK except Π^i_Λ and $\Pi^i_{\bar{\Lambda}}$.

***Definition** 2 (Freshness):* If Π^i_Λ meets the following properties, then we say the instance is *fresh*:

- Π^i_Λ has already accepted the session key SK.
- Prior to acceptance, no participant was asked $Corrupt$ queries.
- Neither Π^i_Λ nor its partners has asked $Reveal$ queries.

***Definition** 3 (Freshness of Session Key):* SK is *fresh* if and only if both Π^i_Λ and $\Pi^i_{\bar{\Lambda}}$ are fresh, where Π^i_Λ and $\Pi^i_{\bar{\Lambda}}$ are partners, and SK is the session key shared between them.

***Definition** 4 (Advantage of Adversary):* Suppose $Succ(\mathcal{A})$ denotes the event that $\mathcal{A}$ makes a $Test(\Pi^i_\Lambda)$ query with the fresh instance Π^i_Λ, and outputs b correctly. The adversary that $\mathcal{A}$ attacking the authenticated key agreement (AKA) protocol Σ is expressed as

$$Adv^{AKA}_\Sigma(\mathcal{A}) = |2Pr[Succ(\mathcal{A})] - 1|.$$

***Definition** 5 (AKA-Secure):* Suppose $Adv^{AKA}_\Sigma(\mathcal{A})$ is a negligible function for any polynomial adversary $\mathcal{A}$, then the protocol Σ is said to be AKA-secure.

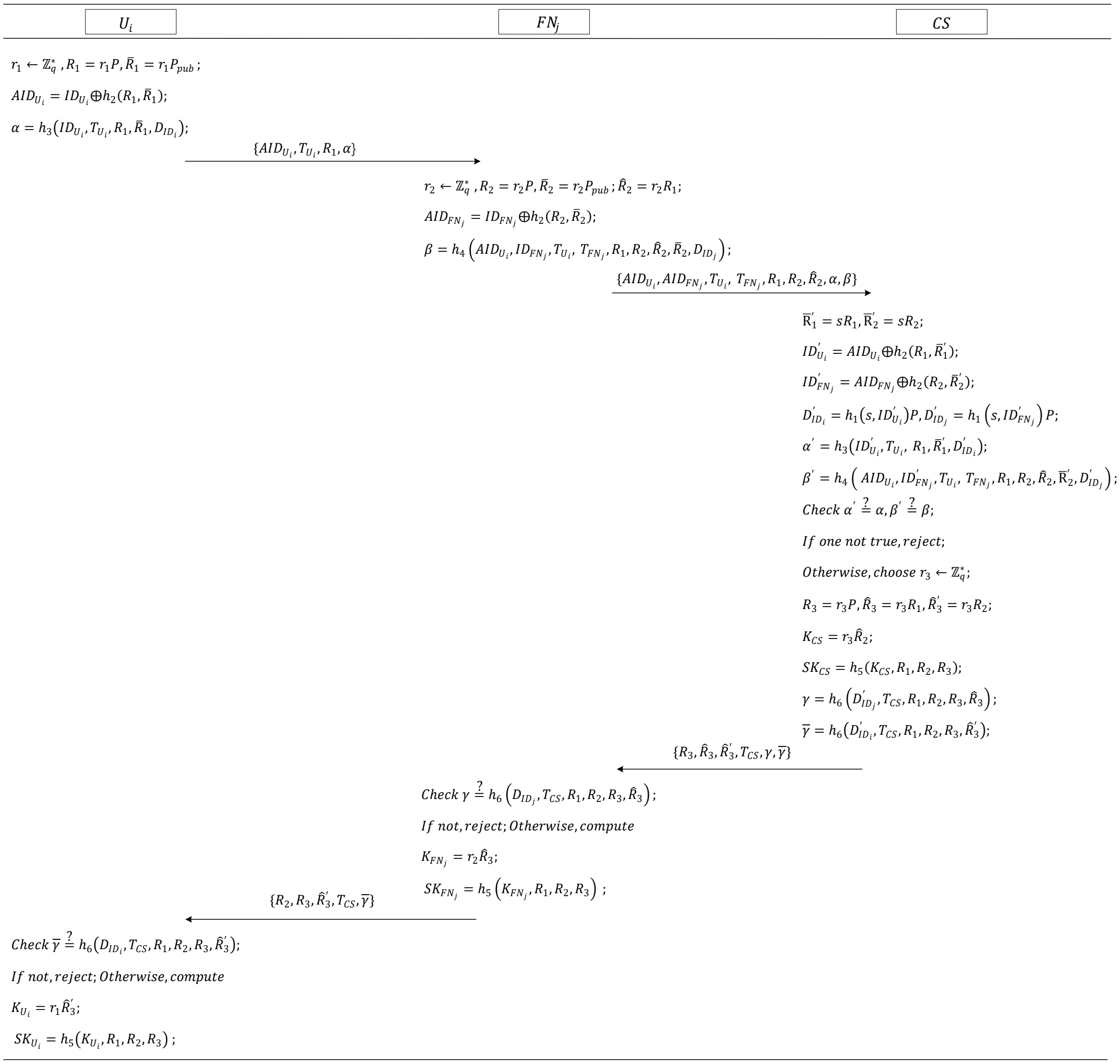
U_i
FN_j
CS
$r_1 \leftarrow \mathbb{Z}_q^*, R_1 = r_1P, \bar{R}_1 = r_1P_{pub};$
$AID_{U_i} = ID_{U_i} \oplus h_2(R_1, \bar{R}_1);$
$\alpha = h_3(ID_{U_i}, T_{U_i}, R_1, \bar{R}_1, D_{ID_i});$
$\{AID_{U_i}, T_{U_i}, R_1, \alpha\}$
$r_2 \leftarrow \mathbb{Z}_q^*, R_2 = r_2P, \bar{R}_2 = r_2P_{pub}; \hat{R}_2 = r_2R_1;$
$AID_{FN_j} = ID_{FN_j} \oplus h_2(R_2, \bar{R}_2);$
$\beta = h_4\left(AID_{U_i}, ID_{FN_j}, T_{U_i}, T_{FN_j}, R_1, R_2, \hat{R}_2, \bar{R}_2, D_{ID_j}\right);$
$\{AID_{U_i}, AID_{FN_j}, T_{U_i}, T_{FN_j}, R_1, R_2, \hat{R}_2, \alpha, \beta\}$
$\bar{\mathrm{R}}_1' = sR_1, \bar{\mathrm{R}}_2' = sR_2;$
$ID_{U_i}' = AID_{U_i} \oplus h_2(R_1, \bar{R}_1');$
$ID_{FN_j}' = AID_{FN_j} \oplus h_2(R_2, \bar{R}_2');$
$D_{ID_i}' = h_1(s, ID_{U_i}')P, D_{ID_j}' = h_1\left(s, ID_{FN_j}'\right)P;$
$\alpha' = h_3(ID_{U_i}', T_{U_i}, R_1, \bar{R}_1', D_{ID_i}');$
$\beta' = h_4\left(AID_{U_i}, ID_{FN_j}', T_{U_i}, T_{FN_j}, R_1, R_2, \hat{R}_2, \bar{\mathrm{R}}_2', D_{ID_j}'\right);$
$Check\ \alpha' \overset{?}{=} \alpha, \beta' \overset{?}{=} \beta;$
$If\ one\ not\ true, reject;$
$Otherwise, choose\ r_3 \leftarrow \mathbb{Z}_q^*;$
$R_3 = r_3P, \hat{R}_3 = r_3R_1, \hat{R}_3' = r_3R_2;$
$K_{CS} = r_3\hat{R}_2;$
$SK_{CS} = h_5(K_{CS}, R_1, R_2, R_3);$
$\gamma = h_6\left(D_{ID_j}', T_{CS}, R_1, R_2, R_3, \hat{R}_3\right);$
$\bar{\gamma} = h_6(D_{ID_i}', T_{CS}, R_1, R_2, R_3, \hat{R}_3');$
$\{R_3, \hat{R}_3, \hat{R}_3', T_{CS}, \gamma, \bar{\gamma}\}$
$Check\ \gamma \overset{?}{=} h_6\left(D_{ID_j}, T_{CS}, R_1, R_2, R_3, \hat{R}_3\right);$
$If\ not, reject; Otherwise, compute$
$K_{FN_j} = r_2\hat{R}_3;$
$SK_{FN_j} = h_5\left(K_{FN_j}, R_1, R_2, R_3\right);$
$\{R_2, R_3, \hat{R}_3', T_{CS}, \bar{\gamma}\}$
$Check\ \bar{\gamma} \overset{?}{=} h_6(D_{ID_i}, T_{CS}, R_1, R_2, R_3, \hat{R}_3');$
$If\ not, reject; Otherwise, compute$
$K_{U_i} = r_1\hat{R}_3';$
$SK_{U_i} = h_5(K_{U_i}, R_1, R_2, R_3);$

Fig. 5. The mutual authentication phase

B. Provable Security

Next, we demonstrate our protocol is AKA-secure under the security model that presented in section V-A.

***Theorem** 1:* Any polynomial adversary $\mathcal{A}$ cannot break the protocol described in section IV with a non-negligible probability.

Proof. If $\mathcal{A}$ wins the protocol with a non-negligible probability ε, then an algorithm $\mathcal{C}$ can be constructed to resolve ECDDH assumption with the probability

$$\begin{aligned}\varepsilon' \quad \geq \quad & \frac{1}{q_s}\Big(\varepsilon - \frac{\sum\limits_{\substack{i=1\\ i\neq 5}}^{6} q_{h_i}^2 + (q_{Se}+q_{Ex})^2}{2q} - \\ & \frac{q_{h_5}}{q} - \frac{2q_{h_2}q_{h_3}}{q^2}\Big).\end{aligned}$$

where q_{h_i} $(1 \leq i \leq 6)$, q_{Se}, q_{Ex}, denote the times of $hash$, $Send$ and $Execution$ queries, respectively.

Given an instance $(P, X = xP, Y = yP, Z = zP)$ of ECDDH assumption, $\mathcal{C}$'s goal is to decide $Z \overset{?}{=} xyP$. $\mathcal{C}$ randomly chooses $s \in \mathbb{Z}_q^*$, calculates $P_{pub} = sP$, and sends the parameters $prms = \{q, \mathbb{G}, P, P_{pub}, h_i(1 \leq i \leq 6)\}$ to $\mathcal{A}$. $\mathcal{C}$ sets the vehicle user U_i's identity, and smart-card as ID_{U_i}, and D_{ID_i} respectively. $\mathcal{C}$ sets the fog node FN_j's identity and smart-card as (ID_{FN_j}, D_{ID_j}). Upon receiving $\mathcal{A}$'s queries, $\mathcal{C}$ responds as follows.

- *Send query.* $\mathcal{C}$ maintains a list L. $\mathcal{A}$ can ask the following $Send$ queries, and $\mathcal{C}$ responds as below.
  - $Send(\Pi_U^i, (FN, START))$: Upon receiving this query, $\mathcal{C}$ selects $r_1 \in \mathbb{Z}_q^*$ randomly, computes $R_1 = r_1P$, $\bar{R}_1 = r_1P_{pub}$, $AID_{U_i} = ID_{U_i} \oplus h_2(R_1, \bar{R}_1)$, $\alpha = h_3(ID_{U_i}, T_{U_i}, R_1, \bar{R}_1, D_{ID_i})$, and sends the login message $M_1 = \{AID_{U_i}, T_{U_i}, R_1, \alpha\}$ to $\mathcal{A}$.
  - $Send(\Pi_{FN}^j, M_1)$: When $\mathcal{C}$ receives this query, it randomly selects $r_2 \in \mathbb{Z}_q^*$, calculates $R_2 = r_2P$, $\hat{R}_2 = r_2R_1$, $\bar{R}_2 = r_2P_{pub}$, $AID_{FN_j} = ID_{FN_j} \oplus h_2(R_2, \bar{R}_2)$, and $\beta = h_4(AID_{U_i}, ID_{FN_j}, T_{U_i}, T_{FN_j}, R_1, R_2, \hat{R}_2, \bar{R}_2, D_{ID_j})$, and sends the message $M_2 =$

  $\{AID_{U_i}, AID_{FN_j}, T_{U_i}, T_{FN_j}, R_1, R_2, \hat{R}_2, \alpha, \beta\}$ to $\mathcal{A}$.
  - $Send(\Pi^k_{CS}, M_2)$: When $\mathcal{A}$ asks this query, $\mathcal{C}$ uses the messages produced in $Send(\Pi^i_U, (FN, START))$ to determine the correctness of α and β. If both of them are correct, $\mathcal{C}$ chooses a number $r_3 \in \mathbb{Z}^*_q$ randomly, computes $R_3 = r_3P$, $\hat{R}_3 = r_3R_1$, $\hat{R}'_3 = r_3R_2$, $K_{CS} = r_3\hat{R}_2$, $SK_{CS} = h_5(K_{CS}, R_1, R_2, R_3)$, $\gamma = h_6(D_{ID_j}, T_{CS}, R_1, R_2, R_3, \hat{R}_3)$, $\bar{\gamma} = h_6(D_{ID_i}, T_{CS}, R_1, R_2, R_3, \hat{R}'_3)$, and sends $M_3 = \{R_3, \hat{R}_3, \hat{R}'_3, T_{CS}, \gamma, \bar{\gamma}\}$ to $\mathcal{A}$. Otherwise, $\mathcal{C}$ rejects $\mathcal{A}$'s query and returns $\perp$.
  - $Send(\Pi^j_{FN}, M_3)$: Upon receiving this query, $\mathcal{C}$ checks the equation $\gamma \overset{?}{=} h_6(D_{ID_j}, T_{CS}, R_1, R_2, R_3, \hat{R}_3)$. If it is not equal, $\mathcal{C}$ terminates $\mathcal{A}$'s query and outputs $\perp$. Otherwise, $\mathcal{C}$ sends $M_4 = \{R_2, R_3, \hat{R}'_3, T_{CS}, \bar{\gamma}\}$ to $\mathcal{A}$.
  - $Send(\Pi^i_U, M_4)$: Upon receiving this query, $\mathcal{C}$ checks the equation $\bar{\gamma} \overset{?}{=} h_6(D_{ID_i}, T_{CS}, R_1, R_2, R_3, \hat{R}'_3)$. If it is not equal, $\mathcal{C}$ terminates $\mathcal{A}$'s query and outputs $\perp$. Otherwise, $\mathcal{C}$ computes $K_{U_i} = r_1\hat{R}'_3$ and $SK_{U_i} = h_5(K_{U_i}, R_1, R_2, R_3)$, the instance Π^i_U is accepted and ended. $\mathcal{C}$ adds (M_1, M_2, M_3, M_4) into the list L.
- *Corrupt query*. $\mathcal{A}$ asks this query with ID_{U_i}, $\mathcal{C}$ responds as follows.
  - Upon receiving a query of $Corrupt(ID_{U_i}, Smart\text{-}Card)$, $\mathcal{C}$ returns D_{ID_i} to $\mathcal{A}$.
- $Execute(\Pi^i_U, \Pi^j_{FN}, \Pi^k_{CS})$. On receiving this query, $\mathcal{C}$ recovers (M_1, M_2, M_3, M_4) from the list L and returns the messages (M_1, M_2, M_3, M_4) to $\mathcal{A}$.
- $Reveal(\Pi^i_\Lambda)$. When $\mathcal{A}$ makes the inquiry, if Π^i_Λ is accepted, then $\mathcal{C}$ sends the session key SK to $\mathcal{A}$. Otherwise, $\mathcal{C}$ outputs $\perp$.
- *Test query.* When $\mathcal{A}$ asks the $Test(\Pi^i_\Lambda)$ query , $\mathcal{C}$ chooses a random $\tau \in \{0,1\}$. If $\tau = 1$, $\mathcal{C}$ returns SK to $\mathcal{A}$. Otherwise, $\mathcal{C}$ randomly chooses a number ν and sends ν to $\mathcal{A}$, where the size of ν is the same as that of SK.

This proof consists of four games $G_i (i = 0, 1, 2, 3)$. Let $\mathcal{E}_i$ indicate that $\mathcal{A}$ correctly guesses the value of τ in game G_i

Game G_0. This game simulates the original attack. In this game, all queries are executed in accordance with the protocol specification. Thus

$$\varepsilon = |2Pr[\mathcal{E}_0] - 1|. \tag{1}$$

Game G_1. This game simulates hash oracles $h_i (1 \leq i \leq 6)$, and $\mathcal{C}$ maintains the lists L_{h_i}. Upon receiving $\mathcal{A}$'s $h_i(M)$ query, $\mathcal{C}$ searches L_{h_i} list, and sends $h_i = h_i(M)$ to $\mathcal{A}$ if there is a record (M, h_i) in L_{h_i}. Otherwise, $\mathcal{C}$ chooses a random value h and returns h to $\mathcal{A}$. For other queries, $\mathcal{C}$ simulates the real attacks and returns the corresponding value to $\mathcal{A}$. We can know that this game is perfectly indistinguishable from game G_0. Thus,

$$Pr[\mathcal{E}_1] = Pr[\mathcal{E}_0]. \tag{2}$$

Game G_2. This game simulates various queries as well as game G_1. The difference is that $\mathcal{C}$ will terminate all instances when the output of $h_i (i \neq 5)$ or the copy of messages (M_1, M_2, M_3, M_4) has a collision. From the birthday paradox, the probability that the output of a hash h_i will collide is at most $q^2_{h_i}/(2q)$. The numbers r_1, r_2, and r_3 are simulated, so they're uniformly randomized, thus the probability that the output of the copy (M_1, M_2, M_3, M_4) will collide is at most $(q_{Se} + q_{Ex})^2/(2q)$. It follows that

$$|Pr[\mathcal{E}_2] - Pr[\mathcal{E}_1]| \leq \frac{\sum\limits_{\substack{i=1 \\ i \neq 5}}^{6} q^2_{h_i} + (q_{Se} + q_{Ex})^2}{2q}. \tag{3}$$

Game G_3. This game modifies $Send$ query. Upon receiving $\mathcal{A}$'s $Send$ queries, $\mathcal{C}$ chooses an instance $(\Pi^i_U, \Pi^j_{FN}, \Pi^k_{CS})$ randomly, and responds as follows.

- Upon receiving $\mathcal{A}$'s $Send(\Pi^i_U, (FN, START))$ query, $\mathcal{C}$ calculates $R_1 = X$, $\bar{R}_1 = sR_1$, and sets the value of AID_{U_i}, α, T_{U_i} as the method in game G_2. At last, $\mathcal{C}$ sends the message $M_1 = \{AID_{U_i}, T_{U_i}, R_1, \alpha\}$ to $\mathcal{A}$.
- Upon receiving $\mathcal{A}$'s $Send(\Pi^j_{FN}, M_1)$ query, $\mathcal{C}$ sets $R_2 = Y$, $\bar{R}_2 = sB, \hat{R}_2 = Z$, and computes AID_{FN_j}, β as the method of game G_2. $\mathcal{C}$ sends the message $M_2 = \{AID_{U_i}, AID_{FN_j}, T_{U_i}, T_{FN_j}, R_1, R_2, \hat{R}_2, \alpha, \beta\}$ to $\mathcal{A}$.
- Upon receiving $\mathcal{A}$'s $Send(\Pi^k_{CS}, M_2)$ query, $\mathcal{C}$ chooses a random number $r_3 \in \mathbb{Z}^*_q$, computes $R_3 = r_3P$, $\hat{R}_3 = r_3R_1, \hat{R}'_3 = r_3R_2$, and calculates $(\gamma, \bar{\gamma})$ as the method of game G_2. $\mathcal{C}$ sets $K_{CS} = r_3\hat{R}_2$ and computes $SK_{CS} = h_5(K_{CS}, R_1, R_2, R_3)$. $\mathcal{C}$ stores (r_3, R_3) on the list L_{CS} and sends $M_3 = \{R_3, \hat{R}_3, \hat{R}'_3, T_{CS}, \gamma, \bar{\gamma}\}$ to $\mathcal{A}$.
- Upon receiving $\mathcal{A}$'s $Send(\Pi^j_{FN}, M_3)$ query, $\mathcal{C}$ looks up the list L_{CS} for (r_3, R_3). $\mathcal{C}$ sets $K_{FN_j} = r_3\hat{R}_2$ and computes $SK_{FN_j} = h_5(K_{FN_j}, R_1, R_2, R_3)$. $\mathcal{C}$ returns $M_4 = \{R_2, R_3, \hat{R}'_3, T_{CS}, \bar{\gamma}\}$ to $\mathcal{A}$.
- Upon receiving $\mathcal{A}$'s $Send(\Pi^i_U, M_4)$ query, $\mathcal{C}$ looks up the list L_{CS} for(r_3, R_3). $\mathcal{C}$ sets $K_{U_i} = r_3Z$, computes $SK_{U_i} = h_6(K_{U_i}, R_1, R_2, R_3)$ and aborts the instance.

If there is a differentiator $\mathcal{D}$, and $\mathcal{D}$ can distinguish G_3 from G_2 successfully, then $\mathcal{C}$ could solve the ECDDH problem by calling $\mathcal{A}$ as a subroutine. According to the above description of game G_2 and G_3, $\mathcal{C}$ simulates all the above queries but don't the value of r_1, r_2, r_3. If $r_3Z = r_3xyP$, i.e., $Z = xyP$, the differentiator interacts with game G_2, and $\mathcal{C}$ outputs 1. Otherwise, the differentiator interacts with game G_3, and $\mathcal{C}$ outputs 0.

The differentiator chooses an instance with the probability of $1/q_{Se}$. Thus,

$$(1/q_{Se})|Pr[\mathcal{E}_3] - Pr[\mathcal{E}_2]| \leq \varepsilon'.$$

It follows that

$$|Pr[\mathcal{E}_3] - Pr[\mathcal{E}_2]| \leq q_{Se}\varepsilon'. \tag{4}$$

In game G_3, the value of $K_{U_i} = K_{FN_j} = K_{CS} = r_3Z$ is random and independent of x, y. $\mathcal{A}$ can't distinguish between SK and a random number unless the following events occur.

Let $E_i (1 \leq i \leq 3)$ denote the following evens.

- E_1: $\mathcal{A}$ has asked a h_5 query with messages (r_3Z, R_1, R_2, R_3). It's easy to figure out $Pr[E_1] = q_{h_5}/q$.

- E_2: $\mathcal{A}$ impersonated the vehicle user and successfully forged the message $M_1 = \{AID_{U_i}, T_{U_i}, R_1, \alpha\}$. In order to forge successfully, $\mathcal{A}$ must correctly calculate the values of AID_{U_i} and α. $\mathcal{A}$ is allowed to ask $Corrupt(ID_{U_i})$ query. However, the value of $\bar{R}_1$ can't be computed because x is an unknown number. Thus,

$$Pr[E_2] \leq (q_{h_2}/q) \cdot (q_{h_3}/q) = (q_{h_2} q_{h_3})/q^2.$$

- E_3: $\mathcal{A}$ impersonated the fog node and successfully forged the message M_2 . Similar to E_2, we have

$$Pr[E_3] \leq (q_{h_2}/q) \cdot (q_{h_3}/q) = (q_{h_2} q_{h_3})/q^2.$$

Hence,

$$Pr[\mathcal{E}_3] \leq \frac{1}{2} + \frac{q_{h_5}}{q} + \frac{2q_{h_2}q_{h_3}}{q^2}. \tag{5}$$

From (1)-(5), we have

$$\varepsilon \leq \frac{\sum\limits_{\substack{i=1 \\ i\neq 5}}^{6} q_{h_i}^2 + (q_{Se}+q_{Ex})^2}{2q} + \frac{q_{h_5}}{q} + \frac{2q_{h_2}q_{h_3}}{q^2} + q_s\varepsilon'.$$

Thus,

$$\varepsilon' \geq \frac{1}{q_s}\Big(\varepsilon - \frac{\sum\limits_{\substack{i=1 \\ i\neq 5}}^{6} q_{h_i}^2 + (q_{Se}+q_{Ex})^2}{2q} - \frac{q_{h_5}}{q} - \frac{2q_{h_2}q_{h_3}}{q^2}\Big).$$

C. Analysis of Security Requirements

Next, we prove our protocol meets the security requirements represented in III-C.

- **Mutual authentication:** From the proof of theorem 1, we can see that no polynomial adversary has the ability to successfully forge a legal login or response message. Hence, the participants could authenticate each other by verifying whether their received message is valid or not. So, the proposed protocol could achieve mutual authentication.
- **Session key agreement:** According to the protocol that represented in IV-D, all the participants can compute the same value $K = r_1 r_2 r_3 P$, and the common session key $SK = h_5(K, r_1P, r_2P, r_3P)$. Hence, the AKA protocol can achieve session key agreement.
- **User anonymity:** By the protocol described in IV-D, the identity ID_{U_i} of the vehicle user U_i is hidden in $AID_{U_i} = ID_{U_i} \oplus h_2(R_1, \bar{R}_1)$. To extract ID_{U_i} from AID_{U_i}, the adversary has to calculate $\bar{R}_1 = r_1 P_{pub}$ from $R_1 = r_1 P$, i.e., the adversary must solve the problem of ECDL. However, the ECDL is intractable, our protocol provides user anonymity.
- **Un-traceability:** By the description of section IV-D, the participants, i.e., U_i, FN_j and CS respectively choose the random numbers r_1, r_2, r_3 to computer $R_1 = r_1P$, $R_2 = r_2P$ and $R_3 = r_3P$. In addition, the timestamps are dynamic in the proposed protocol. Hence, the adversary is unable to trace the participants' behavior and our protocol can support un-traceability.
- **Perfect forward secrecy:** Assume an adversary steals the smart-card, and intercepts messages $R_1 = r_1P, R_2 = r_2P, R_3 = r_3P$. In order to derive the value of $SK = h_5(K_{U_i}, R_1, R_2, R_3)$, the adversary has to compute $K_{U_i} = r_1r_2r_3P$, i.e., it must solve the problem of ECCDH. Since ECCDH assumption is intractable, our protocol provides perfect forward secrecy.
- **No verifier table:** By the protocol described in IV, participants do not need to save the verifier table, they just need to hold their own private key, which is used to authenticate with other participants. Thus, the proposed protocol can resist stolen-verifier attack.
- **Resistance of known session key attack:** According to the protocol described in IV-D, the session keys $SK = h_5(K, R_1, R_2, R_3)$ $(K = r_1r_2r_3P)$ are different in each session as r_1, r_2, r_3 are random numbers. Thus, even if a session key is leaked, it can not affect the privacy of other session keys.
- **Resistance of man-in-the-middle attack:** Suppose $\mathcal{A}$ knows ID_{U_i} and ID_{FN_j}. The goal of $\mathcal{A}$ is to forge valid messages (M_1, M_2, M_3, M_4). To forge a valid M_1, $\mathcal{A}$ selects a number $r_1' \in \mathbb{Z}_q^*$ randomly, computes $R_1' = r_1'P$, $\bar{R_1}' = r_1'P_{pub}$, $AID_{U_i}' = ID_{U_i} \oplus h_2(R_1', \bar{R_1}')$. However, it is difficult for $\mathcal{A}$ to calculate the value of α without D_{ID_i}. Similarly, it is difficult for $\mathcal{A}$ to forge β without D_{ID_j}. Thus, $\mathcal{A}$ cannot calculate M_2. In addition, $\mathcal{A}$ cannot generate M_3 and M_4 without CS's private key s. Thus, our protocol could against man-in-the-middle attack.
- **Resistance of replay attack:** By our protocol described in section IV-D, these timestamps $(T_{U_i}, T_{FN_j}, T_{CS})$ are added to the authentication process. Due to the freshness of $(T_{U_i}, T_{FN_j}, T_{CS})$, the participants (e.g., U_i, FN_j and CS) can defend against message replay attacks by validating the validity of messages that they received.

VI. Performance Analysis

Next, we present the performance analysis of the protocol described in IV from two aspects: computation cost and communication cost. Moreover, the efficiency comparison between the proposed protocol and the related protocol [18] will be shown in this section.

In our experiments, we choose a q-order group $\mathbb{G}$ with the generator P, where q is a 160-bits prime number, and P is a point selected from the super singular elliptic curve E/F_p : $y^2 = x^3 + 1$ (p is a 512-bits prime number).

A. Analysis of Computation Cost

For computational cost analysis, Table I presents the executing time of some basic operations.

We have tested the above operations using the MIRACL library [43]. The implementations were deployed in a mobile phone and a personal computer, the platforms parameters of which are shown in Table II. The mobile phone is the user,

TABLE I
THE EXECUTING TIME OF BASIC OPERATIONS (MS)

Operation	Description	MobilePhone	PersonalComputer
T_{sm}	scalar multiplication	13.405	2.165
T_h	general hash function	0.056	0.007
T_{bp}	bilinear pairing	32.713	5.427

and the personal computer for simulating the servers (e.g., fog and cloud).

TABLE II
SIMULATION PLATFORM

Device	Samsung Galaxy S5	Dell
Operating System	Google Android 4.4.2	Windows 8
CPU	Quad-core 2.45G	I5-4460S 2.90GHz
Memory	2G RAM	4G RAM
Program Language	C	C

Table III and Fig. 6 show the total computation costs of the participants (the user U_i, the fog node FN_j and the cloud server CS).

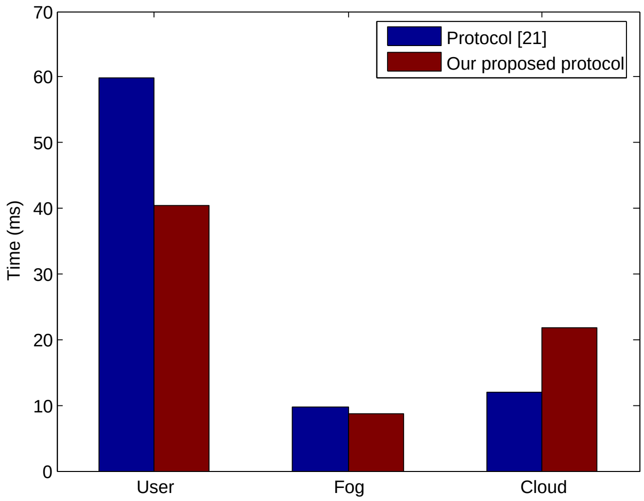

Fig. 6. Comparison of the total computation cost (ms)

For the vehicle user registration phase of protocol [18], both U_i and CS need to perform one hash operation. For the fog node registration phase of [18], CS needs to perform one hash operation. For mutual authentication & key agreement phase of [18], U_i has to execute the following operations: two scalar multiplication, five hash and one bilinear pairing. FN_j needs to perform two scalar multiplication, one bilinear pairing and four hash operations. CS needs to perform two scalar multiplication, one bilinear pairing and nine hash operations. Therefore, the total executing time of U_i, FN_j and CS is $6T_h + 2T_{sm} + T_{bp} \approx 59.859$, $4T_h + 2T_{sm} + T_{bp} \approx 9.785$, and $11T_h + 3T_{sm} + T_{bp} \approx 11.999$, respectively.

For the vehicle user registration phase of our protocol, CS need to perform one general hash and one scalar multiplication operation. For the fog node registration phase, CS needs to perform one general hash and one scalar multiplication operation. For mutual authentication & key agreement phase, U_i executes three scalar multiplication and four hash operations. FN_j executes four scalar multiplication and four hash operations. CS needs to perform the operations of eight scalar multiplication and nine general hash. So, the total executing time of U_i, FN_j and CS is $4T_h + 3T_{sm} \approx 40.439$, $4T_h + 4T_{sm} \approx 8.688$, and $11T_h + 10T_{sm} \approx 21.727$, respectively.

Fig. 6 and Table III show that, for the user U_i, the computation cost of our protocol is lower than that of [18]. For FN_j and CS, our computation cost is almost the same as [18] Thus, our proposed protocol has better performance.

B. Analysis of Communication Cost

Let the length of values in $\mathbb{G}$ and $\mathbb{Z}_q^*$ be expressed by $|\mathbb{G}|$ and $|\mathbb{Z}_q^*|$ respectively. From the above implementation, The sizes of p and q are 512 bits and 160 bits, respectively. So, $|\mathbb{G}| = 1024$ bits and $|\mathbb{Z}_q^*| = 160$ bits. Assume the output size of h_5 is 256 bits, and the size of timestamps is 32 bits, denoted by $|T|$. Table IV shows the comparison of communication costs.

In mutual authentication & key agreement phase, for protocol [18], the communication costs of the vehicle user U_i, the fog node FN_j and the cloud server CS are $|\mathbb{G}| + 2|\mathbb{Z}_q^*| + |T| = 1376$ bits, $4|\mathbb{G}| + 5|\mathbb{Z}_q^*| + 3|T| = 4992$ bits and $|\mathbb{G}| + 2|\mathbb{Z}_q^*| + |T| = 1376$ bits respectively. For our protocol, the communication costs of U_i, FN_j and CS are $|\mathbb{G}| + 2|\mathbb{Z}_q^*| + |T| = 1376$ bits, $6|\mathbb{G}| + 5|\mathbb{Z}_q^*| + 3|T| = 7040$ bits and $3|\mathbb{G}| + 2|\mathbb{Z}_q^*| + |T| = 3424$ bits, respectively. For [18], it can be seen the total communication costs of U_i, FN_j and CS are 1696 bits, 5152 bits and 1696 bits respectively. And for our protocol, the total communication costs of U_i, FN_j and CS are 1696 bits, 7200 bits and 3744 bits respectively.

Table IV presents that, in terms of U_i, the communication cost in our proposed protocol is almost the same as that in [18]. The communication costs of FN_j and CS in our protocol are slightly higher than that of [18]. However, the cloud server and fog node have powerful data storage and processing capabilities. Therefore, our protocol could achieve good communication efficiency and is practical in fog-based VANETs.

VII. CONCLUSION

In the modern and smart society, there will be more internet and interconnected vehicles and devices that underpin the VANETs, ITS or smart city. Hence, ensuring security in VANETs is one of several topics of ongoing interest and urgency.

In this paper, we present an AKA protocol designed to facilitate secure communication in fog-based VANETs. Given the importance of security design, we prove the security of the protocol in random oracle model. We also evaluate the performance of the protocol to demonstrate its utility.

There are, however, a number of potential research extensions in this work. For example, we intend to extend the protocol to allow secure group communication between different vehicles, devices and fog nodes between VANETs located in the same county (e.g. Bexar County in San Antonio, Texas), city (e.g. Austin, San Marco and San Antonio) or state

TABLE III
COMPARISON OF COMPUTATION COSTS (MS)

Protocols	Computational cost of U_i	Computational cost of FN_j	Computational cost of CS
[18]	$6T_h + 2T_{sm} + T_{bp} \approx 59.859$	$4T_h + 2T_{sm} + T_{bp} \approx 9.785$	$11T_h + 3T_{sm} + T_{bp} \approx 11.999$
Our proposed protocol	$4T_h + 3T_{sm} \approx 40.439$	$4T_h + 4T_{sm} \approx 8.688$	$11T_h + 10T_{sm} \approx 21.727$

TABLE IV
COMPARISON OF COMMUNICATION COSTS (BITS)

Protocol	Communicational cost of U_i	Communicational cost of FN_j	Communicational cost of CS
[18]	$\lvert\mathbb{G}\rvert + 4\lvert\mathbb{Z}_q^*\rvert + \lvert T\rvert$=1696	$4\lvert\mathbb{G}\rvert + 6\lvert\mathbb{Z}_q^*\rvert + 3\lvert T\rvert$=5152	$\lvert\mathbb{G}\rvert + 4\lvert\mathbb{Z}_q^*\rvert + \lvert T\rvert$=1696
Our proposed protocol	$\lvert\mathbb{G}\rvert + 4\lvert\mathbb{Z}_q^*\rvert + \lvert T\rvert$=1696	$6\lvert\mathbb{G}\rvert + 6\lvert\mathbb{Z}_q^*\rvert + 3\lvert T\rvert$=7200	$3\lvert\mathbb{G}\rvert + 4\lvert\mathbb{Z}_q^*\rvert + \lvert T\rvert$=3744

(e.g. Texas). We also intend to implement a prototype of the protocol (or its extension) in a real-world application, so that we can more extensively evaluate its real-world utility.

REFERENCES

[1] L. Zhang, X. Men, K.-K. R. Choo, Y. Zhang, and F. Dai, "Privacy-preserving cloud establishment and data dissemination scheme for vehicular cloud," *IEEE Transactions on Dependable and Secure Computing*, no. 1, pp. 1–1, 2018.

[2] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, "Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response," *IEEE Transactions on Computers*, vol. 65, no. 8, pp. 2562–2574, 2016.

[3] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *Journal of Network and Computer Applications*, vol. 40, pp. 325–344, 2014.

[4] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2017.

[5] X. Chen, X. Huang, J. Li, J. Ma, W. Lou, and D. S. Wong, "New algorithms for secure outsourcing of large-scale systems of linear equations," *IEEE transactions on information forensics and security*, vol. 10, no. 1, pp. 69–78, 2015.

[6] Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 767–778, 2017.

[7] L. Zhang, "OTIBAAGKA: a new security tool for cryptographic mix-zone establishment in vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 12, pp. 2998–3010, 2017.

[8] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Computers & Security*, vol. 72, pp. 1–12, 2018.

[9] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, pp. 13–16, 2012.

[10] H. Huang, X. Chen, Q. Wu, X. Huang, and J. Shen, "Bitcoin-based fair payments for outsourcing computations of fog devices," *Future Generation Computer Systems*, vol. 78, pp. 850–858, 2018.

[11] X. Chen, J. Li, X. Huang, J. Li, Y. Xiang, and D. S. Wong, "Secure outsourced attribute-based signatures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 12, pp. 3285–3294, 2014.

[12] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen, "Vehicular fog computing: A viewpoint of vehicles as the infrastructures," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 6, pp. 3860–3873, 2016.

[13] S. Roy, R. Bose, and D. Sarddar, "A fog-based dss model for driving rule violation monitoring framework on the internet of things," *International Journal of Advanced Science and Technology*, vol. 82, pp. 23–32, 2015.

[14] Z. Hao, E. Novak, S. Yi, and Q. Li, "Challenges and software architecture for fog computing," *IEEE Internet Computing*, vol. 21, no. 2, pp. 44–53, 2017.

[15] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 5, pp. 546–556, 2015.

[16] X. Huang, X. Chen, J. Li, Y. Xiang, and L. Xu, "Further observations on smart-card-based password-authenticated key agreement in distributed systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1767–1775, 2014.

[17] M.-C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics," *Expert Systems with Applications*, vol. 41, no. 4, pp. 1411–1418, 2014.

[18] X. Jia, D. He, N. Kumar, and K.-K. R. Choo, "Authenticated key agreement scheme for fog-driven IoT healthcare system," *Wireless Networks*, pp. 1–14, 2018.

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

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

[21] Y. Sun, X. Lin, R. Lu, X. Shen, and J. Su, "Roadside units deployment for efficient short-time certificate updating in VANETs," *2010 IEEE International Conference on Communications (ICC)*, pp. 1–5, 2010.

[22] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-zones for location privacy in vehicular networks," *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, no. LCA-CONF-2007-016, 2007.

[23] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," *2008 IEEE International Conference on Communications*, pp. 1451–1457, 2008.

[24] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," *The 27th Conference on Computer Communications, INFOCOM 2008*, pp. 246–250, 2008.

[25] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *Annual international cryptology conference*, pp. 213–229, 2001.

[26] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Transactions on vehicular Technology*, vol. 59, no. 4, pp. 1606–1617, 2010.

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

[28] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless networks*, vol. 21, no. 5, pp. 1733–1743, 2015.

[29] Y. Liu, L. Wang, and H.-H. Chen, "Message authentication using proxy vehicles in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 8, pp. 3697–3710, 2015.

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

[31] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1319–1328, 2016.

[32] M. R. Asaar, M. Salmasizadeh, W. Susilo, and A. Majidi, "A secure and efficient authentication technique for vehicular ad-hoc networks," *IEEE*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2902840, IEEE Internet of Things Journal

Transactions on Vehicular Technology, vol. 67, no. 6, pp. 5409–5423, 2018.

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

[34] C. Büttner and S. A. Huss, “A novel anonymous authenticated key agreement protocol for vehicular ad hoc networks,” *2015 International Conference on Information Systems Security and Privacy (ICISSP)*, pp. 259–269, 2015.

[35] L. Dang, J. Xu, X. Cao, H. Li, J. Chen, Y. Zhang, and X. Fu, “Efficient identity-based authenticated key agreement protocol with provable security for vehicular ad hoc networks,” *International Journal of Distributed Sensor Networks*, vol. 14, no. 4, pp. 1 550 147 718 772 545–, 2018.

[36] R. Canetti and H. Krawczyk, “Analysis of key-exchange protocols and their use for building secure channels,” *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 453–474, 2001.

[37] D. He and D. Wang, “Robust biometrics-based authentication scheme for multiserver environment,” *IEEE Systems Journal*, vol. 9, no. 3, pp. 816–823, 2015.

[38] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, “Zipf’s law in passwords,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2776–2791, 2017.

[39] D. Wang, W. Li, and P. Wang, “Two birds with one stone: Two-factor authentication with security beyond conventional bound,” *IEEE Transactions on Dependable & Secure Computing*, vol. 15, no. 4, pp. 708–722, 2018.

[40] Q. Feng, D. He, S. Zeadally, N. Kumar, and K. Liang, “Ideal lattice-based anonymous authentication protocol for mobile devices,” *IEEE Systems Journal*, pp. 1–11, 2018, dOI: 10.1109/JSYST.2018.2851295.

[41] D. He, N. Kumar, H. Wang, L. Wang, K. K. R. Choo, and A. Vinel, “A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network,” *IEEE Transactions on Dependable & Secure Computing*, vol. 15, no. 4, pp. 633–645, 2018.

[42] M. Bellare, D. Pointcheval, and P. Rogaway, “Authenticated key exchange secure against dictionary attacks,” *Tecnologia Electronica E Informatica*, vol. 1807, pp. 139–155, 2000.

[43] “Shamus software ltd., miracl library,” http://www.shamus.ie/index.php?page=home, 2016.

Mimi Ma received her Ph.D. degree in applied mathematics from School of Mathematics and Statistics, Wuhan University in 2018. She is currently a lecturer of the College of Information Science and Engineering, Henan University of Technology. Her main research interests include number theory and cloud computing security.

Debiao He received his Ph.D. degree in applied mathematics from School of Mathematics and S-tatistics, Wuhan University in 2009. He is currently a professor of the School of Cyber Science and Engineering, Wuhan University. His main research interests include cryptography and information security, in particular, cryptographic protocols.

Huaqun Wang received the BS degree in mathematics education from the Shandong Normal University and the MS degree in applied mathematics from the East China Normal University, both in China, in 1997 and 2000, respectively. He received the Ph.D. degree in Cryptography from Nanjing University of Posts and Telecommunications in 2006. He is currently a Professor of Nanjing University of Posts and Telecommunications, China. His research interests include applied cryptography, network security, and cloud computing security.

Neeraj Kumar received his Ph.D. in CSE from Shri Mata Vaishno Devi University, Katra, India. He is currently an Associate Professor in the Department of Computer Science and Engineering, Thapar University, Patiala, India. He has guidedmany students leading toM.E. and Ph.D..He has more than 200 technical research papers in leading journals such as IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, the IEEE TRANSACTIONS ON POWER SYSTEMS, IEEE Transactions on Cloud Computing, IEEE Transaction on Information Forensics and Security, IEEE Transactions on Smart Grid, IEEE SYSTEMS JOURNAL, IEEE Communications Magazine, IEEE Wireless Communications Magazine, the IEEE Network Magazine, and conferences including IEEE ICC, IEEE Globecom etc. His research is supported by Department of Science and Technology, Tata Consultancy Services, and University Grants Commission. His research interests include mobile computing, parallel/distributed computing, multiagent systems, service oriented computing, routing, and security issues in mobile ad hoc, sensor, and mesh networks. He is associate editor of JNCA, Elsevier, IJCS, Wiley and Security and Privacy, Wiley.

Kim-Kwang Raymond Choo (SM’15) received the Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA), and has a courtesy appointment at the University of South Australia. In 2016, he was named the Cybersecurity Educator of the Year - APAC (Cybersecurity Excellence Awards are produced in cooperation with the Information Security Community on LinkedIn), and in 2015 he and his team won the Digital Forensics Research Challenge organized by Germany’s University of Erlangen-Nuremberg. He is the recipient of the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, ESORICS 2015 Best Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society’s Wilkes Award in 2008. He is also a Fellow of the Australian Computer Society, and an IEEE Senior Member.