2018

A Privacy-Preserving Fog Computing Framework for Vehicular Crowdsensing Networks

Jiannan Wei
Nanjing University of Science and Technology, jw903@uowmail.edu.au

Xiaojie Wang
Dalian University of Technology

Nan Li
University of Wollongong, nli@uow.edu.au

Guomin Yang
University of Wollongong, gyang@uow.edu.au

Yi Mu
Fujian Normal University, ymu@uow.edu.au

A Privacy-Preserving Fog Computing Framework for Vehicular Crowdsensing Networks

Abstract

Recently, the study of road surface condition monitoring has drawn great attention to improve traffic efficiency and road safety. As a matter of fact, this activity plays a critical role in the management of the transportation infrastructure. Trustworthiness and individual privacy affect the practical deployment of the vehicular crowdsensing network. Mobile sensing as well as contemporary applications is made use of problem solving. The fog computing paradigm is introduced to meet specific requirements, including mobility support, low latency, and location awareness. The fog-based vehicular crowdsensing network is an emerging transportation management infrastructure. Moreover, the fog computing is effective to reduce the latency and improve the quality of service. Most of the existing authentication protocols cannot help the drivers to judge a message when the authentication on the message is anonymous. In this paper, a fog-based privacy-preserving scheme is proposed to enhance the security of the vehicular crowdsensing network. Our scheme is secure with the security properties, including non-deniability, mutual authentication, integrity, forward privacy, and strong anonymity. We further analyze the designed scheme, which can not only guarantee the security requirements, but also achieve higher efficiency with regards to computation and communication compared with the existing schemes.

Disciplines

Engineering | Science and Technology Studies

Publication Details

Wei, J., Wang, X., Li, N., Yang, G. & Mu, Y. (2018). A Privacy-Preserving Fog Computing Framework for Vehicular Crowdsensing Networks. IEEE Access, 6 43776-43784.

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON SECURITY AND PRIVACY FOR VEHICULAR NETWORKS

Received June 27, 2018, accepted July 24, 2018, date of publication July 31, 2018, date of current version August 28, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2861430

A Privacy-Preserving Fog Computing Framework for Vehicular Crowdsensing Networks

JIANNAN WEI[1], (Member, IEEE), XIAOJIE WANG[2], (Student Member, IEEE), NAN LI[3], GUOMIN YANG[3], (Senior Member, IEEE), AND YI MU[4], (Senior Member, IEEE)

[1]School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China
[2]School of Software, Dalian University of Technology, Dalian 116620, China
[3]Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, Wollongong, NSW 2522, Australia
[4]School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350007, China

Corresponding author: Jiannan Wei (jnwei@njust.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61702268.

ABSTRACT Recently, the study of road surface condition monitoring has drawn great attention to improve the traffic efficiency and road safety. As a matter of fact, this activity plays a critical role in the management of the transportation infrastructure. Trustworthiness and individual privacy affect the practical deployment of the vehicular crowdsensing network. Mobile sensing as well as the contemporary applications are made use of problem solving. The fog computing paradigm is introduced to meet specific requirements, including the mobility support, low latency, and location awareness. The fog-based vehicular crowdsensing network is an emerging transportation management infrastructure. Moreover, the fog computing is effective to reduce the latency and improve the quality of service. Most of the existing authentication protocols cannot help the drivers to judge a message when the authentication on the message is anonymous. In this paper, a fog-based privacy-preserving scheme is proposed to enhance the security of the vehicular crowdsensing network. Our scheme is secure with the security properties, including non-deniability, mutual authentication, integrity, forward privacy, and strong anonymity. We further analyze the designed scheme, which can not only guarantee the security requirements but also achieve higher efficiency with regards to computation and communication compared with the existing schemes.

INDEX TERMS Fog computing, crowdsensing vehicular networks, privacy-preserving, strong anonymity, non-deniability.

I. INTRODUCTION

The road surface condition is considered as a major indicator of road quality. As we know, winter weather always brings along with snow, ice, and freezing rain, all of which when acting alongside poor road surface conditions create situations that are potentially dangerous to people, vehicles, and property. As a result, this is an area where systems for monitoring road conditions are critical to improve road safety [1]. The vehicular crowdsensing network has drawn great attentions during recent years and can provide a safe and comfortable driving experience [1]–[4]. Combining the vehicular communication with the sensing technologies is an advanced vehicular technology. It is promising to detect and deal with the road surface condition using this advanced system [1]. Everyone with mobile devices, including smartphones, smartwatches with embedding sensors can gather the environment information or other users' information around us [1], [2]. This property makes it one of the most important innovations. Particularly, the applications and architectures for both crowdsensing and vehicle-based sensing alongside advanced in cloud computing can do data collection, analysis, processing, transmission and storage efficiently [5], [6].

The could-based architecture is applied in many scenarios/applications for instance smart city [7] and vehicle ad hoc networks(VANETs). Figure 1. shows that the cloud-based architecture consists of smart devices, roadside units(RSUs), and cloud servers. Mobile sensors are embedded in smart devices' and RSUs can link to cloud servers. We use the mobile sensors to collect data while there are anomalies on the road. Then the data are transferred to the cloud server for processing. The cloud-based system is centralized [8]. The smart devices and vehicles are deployed in the networking

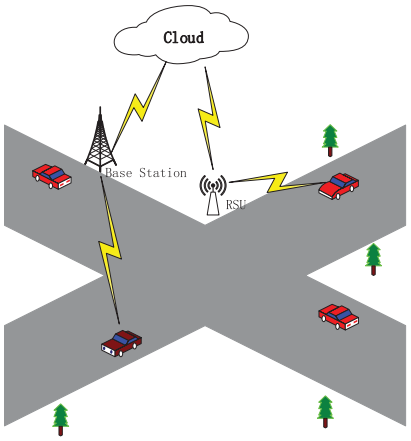

FIGURE 1. Cloud-based architecture.

that can probably lead to crowdsensing. The RSUs play as a role of base station for transferring data to cloud to provide recommendations for processing [9]. The end users are free from the limitation of computation and communication and the storage resources are based on using cloud computing. However, it is too hard for the cloud computing architecture to support user mobility, low latency, and location awareness [8], [10]. The real-time data processing is needed for the approaching cars to offer instant road surface suggestions. When dealing with the crowdsensing data, cloud-based solutions cause several issues such as relaying real-time data to centralized cloud servers which results in increasing bandwidth costs and time delays [11], [12].

The fog computing as well as edge computing [12] can extend the cloud computing and related services to the network edge. The interesting features, including position awareness, low latency, increased mobility [13], and real-time applications processing, provided by fog-based architecture are shown in Figure 2. We can distinguish the fog from the cloud by the dense geographical distribution, its distance to the end users, and its support for mobility [12]. For the fog computing, the data are transmitted to the closed RSU once detected by the sensor, which is different from the cloud-based centralized computing. Then the RSUs will implement the real-time processing and make local decisions [14].

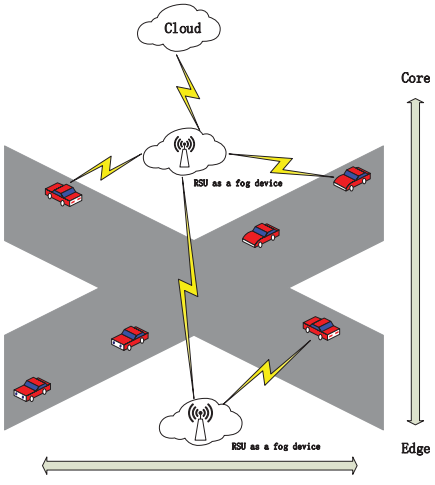

FIGURE 2. Fog-based architecture.

As a matter of fact, vehicular crowdsensing networks allow vehicles to communicate with each other, or vehicles to RSUs, via the sensors equipped in the vehicles. By this kind of communication between the vehicles and RSUs, a lot of attractive comfort services such as weather information and broadcast emergency traffic warning on the road can be provided [15], [16]. Moreover, the security and privacy issues should be addressed before the implementation of the vehicular crowdsensing networks. Otherwise, many problems arise, e.g. the drivers cannot estimate the traffic situation via the received message unless the message has been authenticated. However, if the underlying authentication protocols reveal the real identity of the vehicle, then the location privacy of the vehicle cannot be protected [17]. The security model is shown in Figure 3. We should guarantee the authenticity and integrity of the messages translated in the network. Moreover, users' identity and location should be protected [18], [19]. The fog device itself is vulnerable to the man-in-the-middle attack [20].

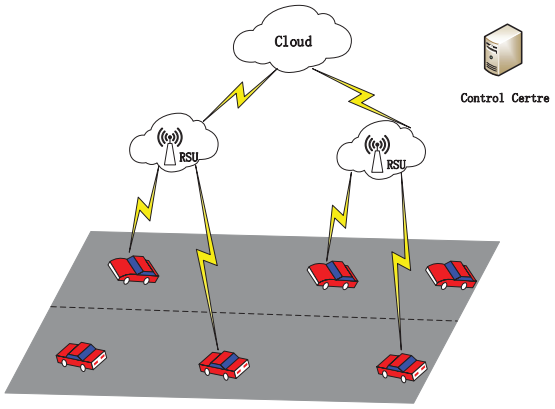

FIGURE 3. Our System Model.

A. RELATED WORK

Much efforts have been directed toward VANETs [2], [3], [6], [11], [21], [22]. There are several mechanisms during the past years. For instance, the silent period [21], creating mix-zones [22], were used to preserve driver privacy. The vehicle mobility can be predicted due to the characteristics of the vehicular network. Furthermore, event the identity of the vehicle was changed, the location of the vehicle can be linked to pseudo identities and then the real identity of the vehicle could be discovered. For the mix-zones, when the approaching vehicles pass the intersection where there is a RSU deployed, the vehicles coordinate with each other and their pseudo identities are changed at the same time.

- **Road Surface Condition Detection** We consider the scenario that mobile sensors are used in detecting the

road surface conditions. With the multiple powerful sensors embedded in, modern devices including GPS systems, accelerometers have made sensing capabilities possible. Mobile sensors are used to detect and report in multiple scenarios. Eriksson *et al*. [23] proposed a mobile sensing app named pothole patrol(P2) to detect and report the road surface condition. Mohan *et al*. [24] also proposed a new approach to improve the P2 system by using wireless sensor networks with the helping of smartphones hardware platform for sensing the surface condition of the road. The proposed protocol uses linkage a data collection system with a database server to store the data. Most of these applications use cloud-based architecture. However, we propose a privacy-preserving protocol for vehicular crowdsensing networks using fog computing.

- **Fog Network Architecture** The fog-based network architecture is a new paradigm that can provide computation, communication, configuration, storage, control, and manage the crucial features, including low response latency, location awareness and geographic distribution [9], [12] between the Internet and terminal devices. The fog nodes located at the edge of the fog networking can communicate with the huge number of self-organized decentralized mobile devices. Moreover, the mobile nodes can collaborate with each other via the fog nodes. There are several fundamental managements include in the fog networking. For example, essential amount of storage is carried out at or nearby the end user rather than storing in the large scale data center. Fog nodes perform a large amount of communication at or near the end-user instead of through the backbone network [25]. Since fundamental managements were carried out, the fog node in the networking should act as a router for its neighbors and adapt to the mobility of the node. Crowdsensing vehicle network is an instantiation of VANET. Therefore, the principles used in VANETs could be the basis for the fog-based crowdsensing vehicle networks [26]. In fog networking, the data collected by the sensor are sent to the network edge devices, routers for processing instead of sending to the cloud servers. Therefore, the fog computing network with a low bandwidth is effective to reduce the traffic data. Moreover, the fog computing minimizes the latency and improves the quality of service. The fog computing reduces the traffic data to the cloud and not delay the computation and communication due to the fog nodes are placed near to data source. The new fog-based computing paradigm supports heterogeneity including access points, edge routers, and enduser devices. It can provide advantages in advertising, entertainment, personal mobile computing, and other applications [27]. Luan *et al.* [28] introduced a distributed fog computing system where the fog servers were deployed in distributed manner by separate owners work.

The RSU who shares the same secret key with the vehicle can create any fake proofs. Public key based protocols can achieve the non-deniability property when digital signature based vehicle authentication mechanism is used. The above reasons and research gap motivated us to develop a new privacy-preserving fog-based protocol that can be used in the vehicular crowdsensing network. Contributions of our work are mainly in the following accepts.

- *Mutual authentication.* Our protocol allows the vehicle and the RSU to mutually recognize and authenticate each other, and is secure against various types of man-in-the-middle and interleaving attacks.
- *Strong user anonymity.* Our protocol can also achieve a strong user anonymity (or unlinkability) property, which ensures that not only the vehicle identity is well-protected, but also a vehicle is unlinkable among different sessions. We utilize the designated verifier signature and the hash chain techniques to achieve this goal.
- *Forward privacy.* Forward privacy ensures that the previous transmitted information cannot be traced if a vehicle is compromised at a later time. Our protocol uses a novel secret updating mechanism to ensure that forward privacy of the vehicle is achieved for different time epoches (or periods).
- *De-synchronization resilience.* The updating of the secret information between the RSU and the vehicle may cause the de-synchronization attack to happen. In our protocol, we use a hash chain and the ''accept then update'' mechanism on the RSU side to make sure the RSU and the vehicle are synchronized.
- *Non-deniability.* One of the contributions of this work is to realize the non-deniability property. The vehicle cannot deny its active involvement in the protocol when there exists a dispute. Also, the RSU was allowed to prove to any third party that the vehicle has indeed participated in an authentication protocol.

Paper Outline: Our paper is organized as follows. We introduce the fog-based vehicular crowdsensing network and review the related work in Section I. Then we give the system model and attack model, which is followed by the security requirements in Section II. We present our new fog-based vehicular crowdsensing protocol in Section III and analyze its security in Section IV. We compare the performance of our protocol with the previous public key based protocols in Section V, and conclude the paper in Section VI.

II. SYSTEM MODELS AND SECURITY REQUIREMENTS

We describe our system model, attack model and the security requirements in this section.

A. SYSTEM MODEL

The road surface condition monitoring system comprise of mobile sensors, e.g., smart devices and vehicles, RSUs as fog devices, a service center(SC) and cloud services. The architecture was shown in Figure 3.

1) Mobile sensors embedded in the smart devices and vehicles generate the signals, time, location and road events i.e., accidents.
2) RSU is an edge device which have storage capacity can extend the cloud service to achieve efficient computational. The RSUs can affect the end users nearby make decisions. The RSUs can do immediate processing when they received a real-time data captured by the mobile sensors.
3) A trusted entity called SC was used to initialize and manage the whole system. Note that SC is a key generation center which cannot access the RSUs and sensors sensitive data. We assume the computation and storage capabilities of the SC is sufficient.
4) The center of the system is cloud servers, all of the system data are stored in the cloud then to be utilized later. We use the fog-based device instead of sending all the data generated by the sensors to the cloud, which can avoid the high latency and high bandwidth cost. The computation was processed by the RSUs. Then the computation results were send to the cloud and the connected devices or vehicles.

B. ATTACK MODEL

In our system, for simplicity, we assume that there is a security channel between the cloud and RSUs. That is, we will treat the RSU and the cloud as a single entity. The RSU and the vehicle are connected via an insecure wireless channel. The information transmitted between the vehicle and the RSU is publicly accessible. We also assume that the decisions made by the vehicle or the RSU is public and known to anybody including the adversary. We only focus our attention to guarantee the security of the data generate from vehicles and then send to RSUs. Our system model is shown in Figure 3.

The message lack of message oriented privacy may result in adversaries release the message and then the receiver may obtain the false message that have been tampered by the adversary. The data can be changed by the malicious adversary for their own benefits. The adversary can control and monitor the whole communication and data transmit through. Particularly, the adversary can change or even replace the message. Furthermore, the attacker can also capture a number of mobile sensors and RSUs. All the data pass through can be analyzed and intercepted by the attacks. Moreover, the RSUs may become attackers and forward the forged messages to the vehicles to make them react in a certain way. The vehicle or smart device could also become malicious which generate false message for his own purpose.

C. SECURITY REQUIREMENTS

In this section, we define the security requirements which are the criteria to evaluate the security of a fog-based vehicular crowdsensing network/VANET protocol. As mentioned above, vehicular crowdsensing network is an instantiation of VANET. We are particularly interested in the following security requirements: mutual authentication, strong anonymity, availability, forward privacy and non-deniability.

- *R1: mutual authentication*: Mutual authentication means the RSU can successfully authenticate the vehicle, and vice versa. vehicle authentication is a basic security requirement for a fog-based vehicle system since the RSU needs to ensure the vehicle it has queried is the real one. RSU authentication is also important in some circumstances, e.g., when the RSU wants to update some information in the vehicle. The vehicle must ensure that the information is from the real RSU.
- *R2: strong anonymity*: As mentioned in the introduction, privacy is an important security requirement for VANETs. The mobile sensors' identities should be hidden during the authentication to protect the sender's private information. Generally, we can separate privacy into weak anonymity and strong anonymity. The former means hiding the identity of the entity, while the latter is also known as untraceability or unlinkability, which means an attacker cannot link multiple communication sessions that involve the same vehicle.
- *R3: availability*: Availability means a VANET system is secure against the Denial-of-Service (DoS) attacks. For VANET systems, we are particularly interested in the security against the de-synchronization attacks between the RSU and the vehicle.
- *R4: forward privacy*: It is also important that the current compromised vehicle information cannot be used to trace the vehicle's previous transmitted information. In this paper, we will focus on forward privacy between different time epoches, which means compromising a vehicle (i.e., obtaining the vehicle's internal state) duing a time epoch does not affect the vehicle's privacy in the previous time epoches.
- *R5: non-deniability*: We should allow the RSU to prove to any third party that the vehicle has indeed participated in an authentication protocol. In particular, the vehicle cannot deny its active involvement in the protocol when a dispute arises.

III. OUR PROPOSED SCHEME

In this section, we present our new fog based VANETs protocol which achieves all the security properties given above. In Table 1 we present the notations that are used in our protocol, which is illustrated in Figure 4.

- **Setup:** Let P denote the generator of a cyclic group of order q. The private and public key pairs of the vehicle and the RSU are $(x, X = xP)$ and $(y, Y = yP)$, respectively, where $x, y \in \mathbb{Z}_q^*$. In our protocol, we use ID_i to denote the identity of the vehicle. Let $h(\cdot)$ and $H(\cdot)$ be cryptographic hash functions. In addition, let K_i denote a symmetric key shared between the RSU and the vehicle i, and t the maximum number of sessions between the RSU and the vehicle in each time epoch. The server maintains a hash chain

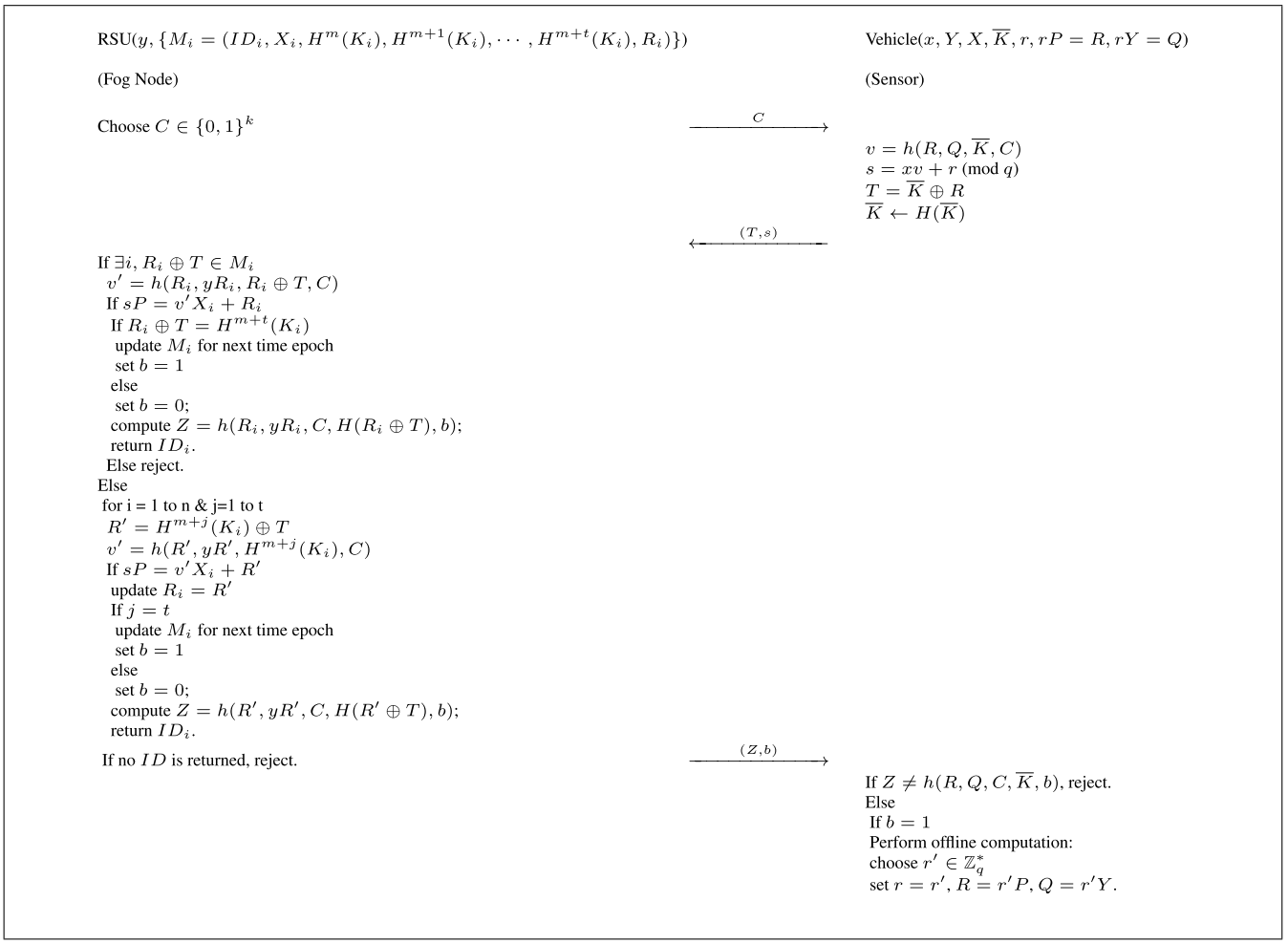

FIGURE 4. Our mutual authentication fog based VANETs protocol with non-deniability.

TABLE 1. Notations used in the protocol.

Symbol	Definition
R	RSU
V	Vehicle
x	Private key of vehicle
X	Public key of vehicle
y	Private key of RSU
Y	Public key of RSU
r	Random number generated by the vehicle
C	A random challenge from the RSU
t	The maximum number of sessions in a time epoch
K_i, $\overline{K}$	Shared secret key between R and V
b	A bit in $\{0, 1\}$
$h(\cdot), H(\cdot)$	Cryptographic hash functions
M_i	A record maintained by the back-end server for vehicle i
$\oplus$	Exclusive-OR

$\{H^m(K_i), H^{m+1}(K_i), \ldots, H^{m+t}(K_i)\}$ for vehicle i and time epoch $\lfloor m/t \rfloor$ where $m = 0$ at the setup (i.e., $H^0(K_i) = K_i$ and $H^{i+1}(K_i) = H(H^i(K_i))$). Also, we use $\overline{K}$ to denote the symmetric key which will be updated by the vehicle in each session, i.e., at the beginning we have $\overline{K} = K_i$.

- **Offline Phase.** At the setup or the end of an epoch, the vehicle randomly chooses $r_i \in \mathbb{Z}_q^*$, and sets $R_i = r_iP$, $Q = r_iY$. This can be performed by the vehicle when it is offline (i.e., not being queried by the RSU). The value of R_i will also be included in the record M_i at the server side once vehicle i has been successfully identified by the RSU (see below for the details).
- **Identification Phase.**
  1) **RSU Challenge:** The RSU randomly chooses a challenge $C \in \{0, 1\}^k$ (k is the security parameter, e.g., 80-bit, 128-bit, 160-bit, etc.) and sends it to the vehicle.
  2) **Vehicle Response:** After receiving C from the RSU, the vehicle first computes $v = h(R, Q, \overline{K}, C)$ and $s = xv + r \pmod q$. The vehicle then sends the pair $(T = \overline{K} \oplus R, s)$ to the RSU and updates $\overline{K} = H(\overline{K})$.
  3) **Vehicle Authentication:** Upon receiving the vehicle's response, the RSU authenticates the vehicle's identity as follows.
     a) For each record M_i in the database, search if $R_i \oplus T \in M_i$ (i.e., $R_i \oplus T$ is in the hash chain).

If such a record is found, then compute $v' = h(R_i, yR_i, R_i \oplus T, C)$ and check whether $sP = v'X_i + R_i$. If the verification is successful, the vehicle ID_i is successfully identified. The RSU checks if the hash chain for the current epoch is used up. If so, update the record M_i to the next epoch and set $b = 1$. Otherwise, set $b = 0$. Compute $Z = h(R_i, yR_i, C, H(R_i \oplus T), b)$ and send (Z, b) to the vehicle.

b) Otherwise, if no $R_i \oplus T$ if found in the database, for $i = 1$ to n and $j = 1$ to t, compute $R' = H^{m+j}(K_i) \oplus T$, $v' = h(R', yR', H^{m+j}(K_i), C)$, and check whether $sP = v'X_i + R'$. If so, the authentication for vehicle ID_i is successful. The RSU updates $R_i \leftarrow R'$, and checks if the hash chain for the current epoch is used up. If so, update the record M_i to the next epoch and set $b = 1$. Otherwise, set $b = 0$. Compute $Z = h(R, yR, C, H(R' \oplus T), b)$ and sends (Z, b) to the vehicle. If no vehicle is identified during the whole loop, the RSU rejects the vehicle.

4) **RSU Authentication:** The RSU should also authenticate itself to the vehicle. After receiving (Z, b), the vehicle checks whether $h(Z) \stackrel{?}{=} h(R, Q, C, \overline{K}, b)$.

- If the equation is true, meaning that the RSU is also successfully authenticated, the vehicle accepts the RSU. If $b = 1$, meaning that the hash chain in the RSU side has been updated to the next epoch, the vehicle performs the *Offline Phase* to choose a new $r' \in \mathbb{Z}_q^*$ and compute $R = r'P, Q = r'Y$.
- Otherwise, the authentication of the RSU is failed, and the vehicle does not perform any action.

IV. SECURITY ANALYSIS

In this section, we will analyze the security of the proposed fog-based vehicle protocol in terms of the security requirements defined in Section III.

A. R1: MUTUAL AUTHENTICATION BETWEEN VEHICLE AND RSU

For the mutual authentication, our protocol can achieve both vehicle authentication and RSU authentication.

1) VEHICLE AUTHENTICATION

Our protocol uses the Schnorr signature [29] for vehicle authentication. In our protocol, the RSU sends a fresh challenge C to the vehicle in each session, and the vehicle sends back a response which contains an anonymized Schnorr signature (T, s). After receiving the response, the RSU checks whether a valid Schnorr signature (R_i, s) can be recovered from the response. If the vehicle has been authenticated successfully before for the same time epoch, then the RSU has already had the value of R_i, and it can locate this value by a search over database. Otherwise, the RSU has to go through the hash chain for each vehicle to locate a value R' such that (R', s) form a valid siganture. Since the Schnorr signature is existentially unforgeable under chosen message attacks [30], no one is able to forge a valid signature without knowing the private signing key. Also, since the RSU uses a fresh nonce C as a challenge in each session, the attack cannot replay a signature, which has been used by the vehicle before, in a new session. Therefore, combining the unforgeability of the Schnorr signature and the challenge-response mechanism, vehicle authentication can be achieved.

2) RSU AUTHENTICATION

In the case of authenticating the RSU, after receiving (Z, b) from the RSU, the vehicle computes $h(R, Q, C, H(\overline{K}), b)$ and checks whether it equals to Z. If the RSU is the real one, i.e., it knows the RSU's private key y, then it can compute $yR = rY = Q$. Otherwise, due to the difficulty of the Diffie-Hellman problem, an attacker is not able to calculate the value of Q. Also, since the value $\overline{K}$ is updated by the vehicle in each session, it serves as a nonce to prevent the replay attacks.

B. R2: STRONG ANONYMITY OF THE VEHICLE

Our protocol can guarantee strong anonymity of the vehicle, which implies vehicle anonymity and untraceability. During the execution of the anonymous authentication protocol in the Identification Phase, vehicle the response T is never repeated in different sessions although the same R is used during a time epoch (i.e., t sessions). This is achieved by masking R using a symmetric key $\overline{K}$ shared between the RSU and the vehicle. Since $\overline{K}$ is only known by the RSU and the vehicle and is updated in each session using the hash chain, the value of T is independent in different sessions if we treat the hash function as a random function. Also, due to the uniqueness of $\overline{K}$ and C in each session, the values of v and s are also diffferent between different sessions. Therefore, only the RSU who is a designated verifier can recover and verify the signature, while from the advresary's view point, T and s are just fresh random values in each session.

C. R3: AVAILABILITY

As we have mentioned before, many VANETs authentication schemes which update the secret information between the RSU and the vehicle are subject to the de-synchronization (or DoS) attack. In our protocol, we need to guarantee the synchronization of R and $\overline{K}$ between the RSU and the vehicle.

The value of R is changed for each session during a time epoch. Therefore, once a vehicle is recognized and authenticated by the RSU, the value of R will be stored by the RSU, and for the rest of the time epoch, the value of R remains unchanged and hence is always synchronized. When the vehicle updates the value of R at the end of an epoch, it becomes de-synchronized with the RSU. Nevertheless, the RSU will discover the unsynchronization during the next

identification session, and update the value of R once the vehicle is authenticated.

The value of $\overline{K}$ is updated by the vehicle in each session, no matter the session is successfully completed or not. However, since the RSU keeps a long hash chain, as long as $\overline{K}$ is within the hash chain, the vehicle and the RSU remain synchronized. Also, during the identification process, when the RSU detects that the entire hash chain has been used up, it will update the hash chain for the next time epoch. We should note that the RSU will update the hash chain only when the vehicle has successfully passed the authentication, which means the vehicle has updated $\overline{K}$ to the first element of the next hash chain.

D. R4: FORWARD PRIVACY

Forward privacy means that even if a vehicle is compromised, its privacy in the previous authentication sessions is still well preserved. Our proposed protocol can achieve forward privacy for all the authentication sessions belonging to the previous time epochs when a vehicle is compromised.

When a vehicle is compromised during a time epoch, the adversary is able to obtain all the current state information of the vehicle which includes $(x, Y, X, \overline{K}, r, R = rP, Q = rY)$. Since the vehicle updates the value of $\overline{K}$ in each session using a hash-chain, due to the one-wayness of the hash function, from $\overline{K} = H^i(K)$, the adversary cannot derive the previous keys $H^j(K)$ for $j = 0, 1, \cdots, i - 1$. Also, since the values of (r, R, Q) are updated at the end of a time epoch, the adversary is not able to obtain such values for the previous time epoches. Therefore, the adversary is not able to trace the authentication sessions of the vehicle in the previous time epochs.

However, we should note that our proposed protocol cannot ensure the forward privacy of a vehicle within one time epoch. Given the state information $(x, Y, X, \overline{K}, r, R = rP, Q = rY)$ of a vehicle, since the value of R is changed during a time epoch, the adversary can compute $\overline{K}' = T' \oplus R$ for some T' appeared in a previous authentication session s. If $\overline{K} = H^\ell(\overline{K}')$ for some integer ℓ, then the adversary knows that the vehicle is invloved in the session s.

E. R5: NON-DENIABILITY

Non-deniability ensures that a vehicle cannot deny that it has involved in an authentication session. Such a property cannot be achieved using symmtric key techniques. Our protocol can achieve this property due to the use of the Schnorr signature for vehicle authentication. Since the Schnorr signature is existentially unforgeable [30], no one except the vehicle is able to create a valid signature. In order to prove that a vehicle is involved in an identification session, the RSU can release $R, Q, \overline{K}$ that occurred in a successfully authenticated session with the communication transcript (C, T, s) to a third party who can check the validity of the signature via the equations $sP = h(R, Q, \overline{K}, C)X + R$ and $T = \overline{K} \oplus R$. We should note that the RSU does not need to disclose its private key y in order to prove the involvement of a vehicle in a particular session.

V. PERFORMANCE ANALYSIS

In this section we analyze the performance of our protocol and compare it with some public key based protocols. Since we can assume the service server connected to the RSU is a powerful device, we will mainly focus on the performance of the vehicle.

A. COMPUTATION AND COMMUNICATION COST

In terms of the computation cost, the vehicle needs to perform $2t$ exponentiation (i.e., scalar multiplication if implemented using ECC) operations for each time epoch (i.e., t sessions). For each online session, the vehicle needs to do 3 hash operations. Therefore, for each time epoch, the vehicle needs to do a total of $2t$ exponentiation operations and $3t$ hash operations.

For the communication cost, our protocol requires 3 rounds for mutual authentication in each session. The total length of the messages exchanged between the RSU and the vehicle is $(k + 3 * |P| + 1)$ bits. Here we assume that both of the hash functions have a output length of $|P|$ (i.e., the length of a group element). For ECC, we have $|P| = 2k$, so the total length of the exchanged messages is $7k + 1$ bits.

B. COMPARISON

We compare the security and the performance of our protocol with some existing public key based protocols in Table 3 and Table 4, respectively. From the tables, we can see that our protocol provides strong security but incurs less computation overhead. In particular, our protocol requires less linear number of exponentiation operations in each time epoch.

TABLE 2. Operation running time.

Operation	Running Time	Descriptions
h	0.065ms	Time for a hash operation
e	1.6s	Time for a scalar multiplication

TABLE 3. Security comparison among public key based protocols.

Protocol	[33] (P2)	[34] (P2)	Our scheme
Mutual authentication	×	×	√
Strong anonymity	√	√	√
Availability	√	√	√
Forward privacy	√	×	√
Non-deniability	√	√	√

TABLE 4. Performance comparison among public key based protocols.

Protocol	[33] (P2)	[34] (P2)	Our scheme
Computation (per time epoch)	$3te + 3th$	$5te$	$2te+3th$
Communication round (per session)	2	3	3
Message length (per session, k=80)	800b	800b	561b

Notations: e – scalar multiplication, h – hash function evaluation, t – number of sessions in each epoch, b – bit

TABLE 5. Tag computation time ($t = 10$).

Number of Sessions	10	20	30	40	50
[33] (P2)	48.00	96.00	144.01	192.01	240.01
[34] (P2)	80	160	240	320	400
Our scheme	32.00	64.00	96.01	128.01	168.01

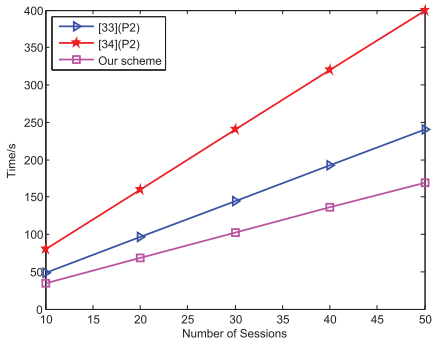

FIGURE 5. Tag computation time (t = 10).

According to the running time results in [31] and [32], one hash function evaluation requires about 0.065ms, while one exponentiation (i.e., scalar multiplication) operation requires roughly 1.6s. Based on these data, in Table 5 and Figure 5 we compare the accumulated running time of the tag for T sessions where $T = 10, 20, \ldots, 50$. We assume that each time epoch has 10 sessions (i.e., $t = 10$).

VI. CONCLUSION

In this paper, we first reviewed the limitations of the existing cloud based networking. Then we constructed a privacy-preserving protocol for the vehicular crowdsensing network using fog computing. The protocol can achieve all the necessary security requirements including mutual authentication, strong anonymity, availability, forward privacy and non-deniability. The security and performance analysis shows that our protocol achieves strong security. The comparisons of computation and communication cost show that our scheme can achieve better efficiency.

ACKNOWLEDGMENT

The authors wish to thank the reviewers for their helpful comments.

REFERENCES

[1] M. Perttunen *et al.*, "Distributed road surface condition monitoring using mobile phones," in *Proc. Int. Conf. Ubiquitous Intell. Comput.* Berlin, Germany: Springer, 2011, pp. 64–78.

[2] Z. Ning *et al.*, "A cooperative quality-aware service access system for social Internet of vehicles," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2017.2764259.

[3] S. Basudan, X. Lin, and K. Sankaranarayanan, "A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing," *IEEE Internet Things J.*, vol. 4, no. 3, pp. 772–782, Jun. 2017.

[4] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of fog computing and its security issues," *Concurrency Comput., Pract. Exper.*, vol. 28, no. 10, pp. 2991–3005, 2016.

[5] W. Hou, Z. Ning, L. Guo, and X. Zhang, "Temporal, functional and spatial big data computing framework for large-scale smart grid," *IEEE Trans. Emerg. Topics Comput.*, to be published, doi: 10.1109/TETC.2017.2681113.

[6] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 146–152, Jun. 2017.

[7] N. Mitton, S. Papavassiliou, A. Puliafito, and K. S. Trivedi, "Combining cloud and sensors in a smart city environment," *EURASIP J. Wireless Commun. Netw.*, vol. 2012, Dec. 2012, Art. no. 247.

[8] M. Armbrust *et al.*, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[9] I. Stojmenovic, "Fog computing: A cloud to the ground support for smart things and machine-to-machine networks," in *Proc. Australas. Telecommun. Netw. Appl. Conf. (ATNAC)*, Nov. 2014, pp. 117–122.

[10] L. Guo, Z. Ning, W. Hou, X. Hu, and P. Guo, "Quick answer for big data in sharing economy: Innovative computer architecture design facilitating optimal service-demand matching," *IEEE Trans. Automat. Sci. Eng.*, to be published, doi: 10.1109/TASE.2018.2838340.

[11] M. Sookhak *et al.*, "Fog vehicular computing: Augmentation of fog computing using vehicular cloud computing," *IEEE Veh. Technol. Mag.*, vol. 12, no. 3, pp. 55–64, Sep. 2017.

[12] J. Zhang *et al.*, "Energy-latency trade-off for energy-aware offloading in mobile edge computing networks," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2017.2786343.

[13] X. Wang, Z. Ning, and L. Wang, "Offloading in Internet of vehicles: A fog-enabled real-time traffic management system," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2018.2816590.

[14] T. H. Luan, L. Gao, Z. Li, Y. Xiang, G. Wei, and L. Sun. (2015). "Fog computing: Focusing on mobile users at the edge." [Online]. Available: https://arxiv.org/abs/1502.01815

[15] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Comput. Commun.*, vol. 31, no. 12, pp. 2803–2814, 2008.

[16] Z. Ning, X. Wang, X. Kong, and W. Hou, "A social-aware group formation framework for information diffusion in narrowband Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1527–1538, Jun. 2018.

[17] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1711–1720, Mar. 2016.

[18] A. Mednis, A. Elsts, and L. Selavo, "Embedded solution for road condition monitoring using vehicular sensor networks," in *Proc. 6th Int. Conf. Appl. Inf. Commun. Technol. (AICT)*, Oct. 2012, pp. 1–5.

[19] F. Bonomi, "Connected vehicles, the Internet of Things, and fog computing," in *Proc. 8th ACM Int. Workshop Veh. Inter-Netw. (VANET)*, Las Vegas, CA, USA, 2011, pp. 13–15.

[20] L. Zhang, W. Jia, S. Wen, and D. Yao, "A man-in-the-middle attack on 3G-WLAN interworking," in *Proc. Int. Conf. Commun. Mobile Comput. (CMC)*, vol. 1, Apr. 2010, pp. 121–125.

[21] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," in *Proc. Workshop Embedded Secur. Cars*, Nov. 2005.

[22] J. Freudiger, M. Raya, M. Félegyházi, and P. Papadimitratos, "Mix-zones for location privacy in vehicular networks," in *Proc. ACM Workshop Wireless Netw. Intell. Transp. Syst. (WiN-ITS)*, Vancouver, BC, Canada, 2007, pp. 1–7.

[23] J. Eriksson, L. Girod, B. Hull, R. Newton, S. Madden, and H. Balakrishnan, "The pothole patrol: Using a mobile sensor network for road surface monitoring," in *Proc. 6th Int. Conf. Mobile Syst., Appl., Services*, 2008, pp. 29–39.

[24] P. Mohan, V. N. Padmanabhan, and R. Ramjee, "Nericell: Rich monitoring of road and traffic conditions using mobile smartphones," in *Proc. 6th ACM Conf. Embedded Netw. Sensor Syst.*, 2008, pp. 323–336.

[25] M. Chiang. (2016). "Fog networking: An overview on research opportunities." [Online]. Available: https://arxiv.org/abs/1601.00835

[26] L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog: Towards a comprehensive definition of fog computing," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 5, pp. 27–32, Oct. 2014.

[27] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

[28] T. H. Luan, L. X. Cai, J. Chen, X. Shen, and F. Bai, "VTube: Towards the media rich city life with autonomous vehicular content distribution," in *Proc. 8th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Netw.*, Jun. 2011, pp. 359–367.
[29] C. P. Schnorr, "Efficient signature generation by smart cards," *J. Cryptol.*, vol. 4, no. 3, pp. 161–174, 1991.
[30] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 1070. Berlin, Germany: Springer, 1996, pp. 387–398.
[31] S. S. D. Selvi, S. S. Vivek, J. Shriram, S. Kalaivani, and C. P. Rangan, "Identity based aggregate signcryption schemes," in *Proc. INDOCRYPT*, vol. 9. India: Springer, 2009, pp. 378–397.
[32] S. Vaudenay, "On privacy models for RFID," in *Advances in Cryptology—ASIACRYPT* (Lecture Notes in Computer Science), vol. 4833. Kuching, Malaysia: Springer, 2007, pp. 68–87.
[33] N. Li, Y. Mu, W. Susilo, F. Guo, and V. Varadharajan, "Privacy-preserving authorized RFID authentication protocols," in *Proc. Int. Workshop Radio Freq. Identificat., Secur. Privacy Issues*. Cham, Switzerland: Springer, 2014, pp. 108–122.
[34] Y. K. Lee, L. Batina, D. Singelée, and I. Verbauwhede, "Low-cost untraceable authentication protocols for RFID," in *Proc. 3rd ACM Conf. Wireless Netw. Secur.*, 2010, pp. 55–64.

JIANNAN WEI (M'18) received the M.S. degree from Zhengzhou University, China, in 2012, and the Ph.D. degree from the School of Computer Science and Software Engineering, University of Wollongong, Australia. She currently is Assistant Professor with the School of Computer Science and Engineering, Nanjing University of Science and Technology, China. Her major research interests include public key cryptography, vehicular crowdsensing network, privacy-preserving digital signatures, and wireless network security.

XIAOJIE WANG (S'16) received the master's degree from Northeastern University, China, in 2011. She is currently pursuing the Ph.D. degree with the School of Software, Dalian University of Technology, Dalian, China. From 2011 to 2015, she was a Software Engineer at Neusoft Corporation. Her research interests are social computing and network security.

NAN LI received the M.S. and Ph.D. degrees from the School of Computer Science and Software Engineering, University of Wollongong, Australia. He is currently a Research Fellow with the School of Computing and Information Technology, University of Wollongong. His major research interests include applied cryptography, crowdsensing network, privacy-preserving, and wireless network communications.

GUOMIN YANG (SM'17) received the Ph.D. degree in computer science from the City University of Hong Kong in 2009. From 2009 to 2012, he was a Research Scientist at Temasek Laboratories, National University of Singapore. He is currently a Senior Lecturer and ARC DECRA Fellow with the School of Computing and Information Technology, University of Wollongong. His research mainly focuses on applied cryptography and network security.

YI MU (SM'03) received the Ph.D. degree from the Australian National University in 1994. He is currently working with the School of Mathematics and Computer Science, Fujian Normal University, China. His current research interests include information security and cryptography. He is a member of the IACR. He is the Editor-in-Chief of the *International Journal of Applied Cryptography* and serves as an Associate Editor for ten other international journals.