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.2017.2666783, IEEE Internet of Things Journal

A Privacy-preserving Vehicular Crowdsensing based Road surface Condition Monitoring System Using Fog Computing

Sultan Basudan, Xiaodong Lin, Karthik Sankaranarayanan
Faculty of Business and Information Technology, University of Ontario Institute of Technology
Oshawa, Ontario, Canada L1H 7K4
Email: sultan.basudan@uoit.net, {xiaodong.lin, karthik}@uoit.ca

***Abstract*—In the recent past, great attention has been directed towards road surface condition monitoring. As a matter of fact, this activity is of critical importance in transportation infrastructure management. In response, multiple solutions have been proposed which make use of mobile sensing, more specifically contemporary applications and architectures that are used in both crowdsensing and vehicle based sensing. This has allowed for automated control as well as analysis of road surface quality. These innovations have thus encouraged and showed the importance of cloud to provide reliable transport services to clients. Nonetheless, these initiatives have not been without challenges that range from mobility support, locational awareness, low latency as well as geo-distribution. As a result, a new term has been coined for this novel paradigm, called, fog computing. In this paper, we propose a privacy-preserving protocol for enhancing security in vehicular crowdsensing based road surface condition monitoring system using fog computing. At the onset, the paper proposes a certificateless aggregate signcryption scheme (CLASC) that is highly efficient. On the basis of the proposed scheme, a data transmission protocol for monitoring road surface conditions is designed with security aspects such as information confidentiality, mutual authenticity, integrity, privacy as well as anonymity. In analyzing the system, the ability of the proposed protocol to achieve the set objectives and exercise higher efficiency with respect to computational and communication abilities in comparison to existing systems is also considered.**

Keywords*—Fog computing, Road surface condition monitoring System, Security, Certificateless aggregate signcryption

I. INTRODUCTION

The condition of road surfaces is considered as a major indicator of the quality of roads. As a matter of fact, classification of a road as either safe or dangerous, more often than not take into consideration the surface condition of the road. Conventionally, parameters such as potholes, bumps and slipperiness are considered as the distinguishing features of the quality of road surfaces [1]. Notable as well is the fact that surface condition of roads are amongst the major reasons that vehicles get damaged and age faster. In Ontario (Canada), winter weather is known to bring along with it snow, sleet, ice, and freezing rain, among others, all of which when acting alongside poor road surface conditions create situations that are potentially dangerous to motorists, vehicles, people and property [30]. As a result, this is an area where systems for monitoring road conditions are critical to the improvement of safety in roads, lowering accident rates and protection of vehicles from getting damaged as a result of poor surface road conditions.

Municipalities worldwide spend millions of dollars on maintenance and repair of road surfaces [2]. Traditionally, the municipalities engage patrol crews that perform physical examination of road surface conditions with the aim of identifying slippery spots and potholes, etc. Nonetheless, using advanced vehicular technologies especially, vehicular communication combined with sensing technologies, road anomalies can be easily identified and dealt with. This is achieved using an advanced system for monitoring road surface condition [3]. As a matter of fact, advances in sensing technologies such as smartphones and other personal smart devices has allowed the use of sensors in gathering useful information from the environment [1], [2], [3]. This makes it one of the most important innovations for the future.

The technological strides made in mobile communication for instance smartphones, smartwatches, and other personal gadgets (through their inbuilt sensors) has aided in gathering information regarding the environment around us. For example, everyone has a mobile device and gathering data from the user is one of the key elements of future smart cities. As a matter of fact, emphasis is placed on contemporary applications/architectures for both crowdsensing and vehicle based sensing alongside advances in cloud computing allow for data collection, analysis, storage, processing and transmission in an efficient manner.

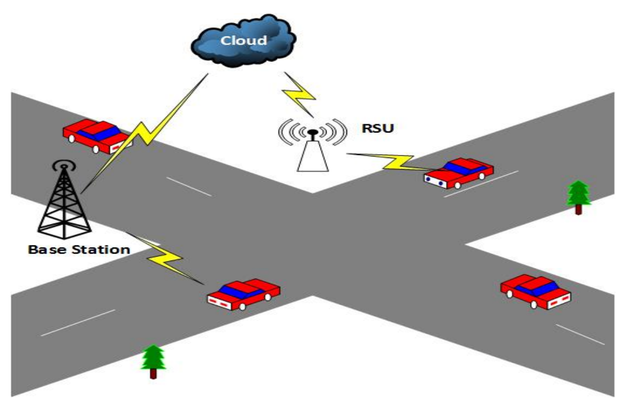
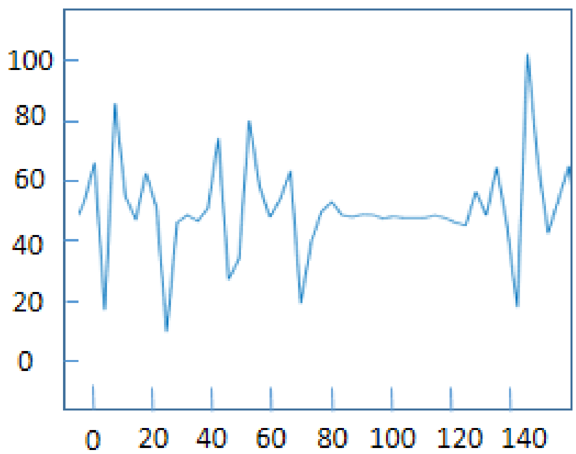


Fig. 1. Cloud based architecture

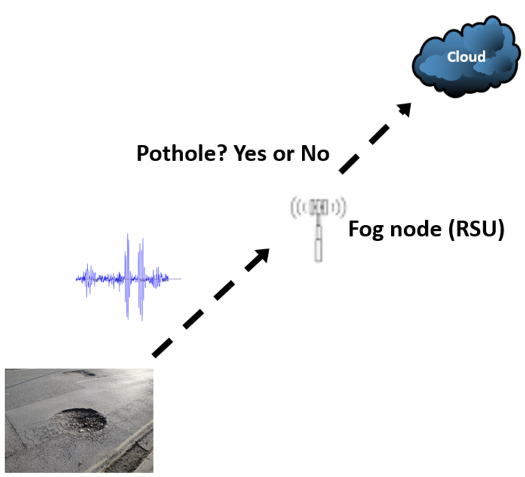
Cloud based architecture as shown in Fig.1 is used by various applications, such as smart city application [33], consists of mobile sensors that could be embedded in either a vehicle or some smart devices/roadside units and linked to cloud servers. Mobile sensors are used to collect data when the vehicle encounters anomalies while on the road as displayed in Fig.2 (a), for example, hitting a pothole. The data is then transferred to a centralized cloud system from where it is processed. The cloud based facility acts as an efficient

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.2017.2666783, IEEE Internet of Things Journal

means through which the integrated system remains up to date while maintaining privacy and security. It is assumed that the applications are deployed such that the vehicles and smart devices can potentially lead to crowdsensing. The roadside units (RSUs) as well as base stations help in relaying data to the cloud for processing and to provide recommendations [4]. For any applications, the approaching cars require real-time data processing in order to be able to offer instant recommendations with regard to the road surface conditions. Nonetheless, solutions that are cloud based and used in dealing with crowdsensing as well as vehicular based sensing data presents a number of issues such as transmission of extensive real-time data to the centralized cloud servers that are prone to time delays and elevated costs of bandwidth.



(a) Accelerometer signals



(b) Detected results at Fog Node (RSU)

Fig. 2. An example of Detected results

Recently, a computer paradigm is emerging, also referred to as fog or edge computing [5]. This is a computing model that stretches cloud computing and related services to the network edge. This offers interesting features by using fog based architecture as represented in Fig.3 including low latency and position awareness, large node, extensive geo-distribution, increased mobility, real-time applications processes, heterogeneity/interoperability, as well as federation [5]. On the contrary though, unlike the globally centralized cloud based systems, once the included mobile sensors detect and generate data, the data is transmitted to the closest RSU, i.e., a fog device [4]. The RSU then does real-time computation in addition to taking local decisions as shown in Fig.2 (b). The results along with recommendations can also be transmitted to other approaching vehicles heading towards the affected region. This system thus achieves low latency as well as reduction in bandwidth costs. We can thus envision a system for measuring road surface conditions with the use of fog computing which allows applications to operate as reasonably as possible to the sensed, actionable and massive information collected via sensors.

Nonetheless, security and privacy issues need to be addressed before its implementation in the Vehicular Ad hoc Networks (VANETs). It is not just message confidentiality that need to be addressed but also the authenticity and integrity of the message. Furthermore, it is important to protect user-related data, including user ID and position, among others. A majority of previously reported literature have paid attention to the transmission of data in VANETs [6], [7], [8], [9], [10]. Nevertheless, the security challenges, particularly with respect to ways through which authenticity and confidentiality can be ensured with regard to the road event reported are still to be explored.

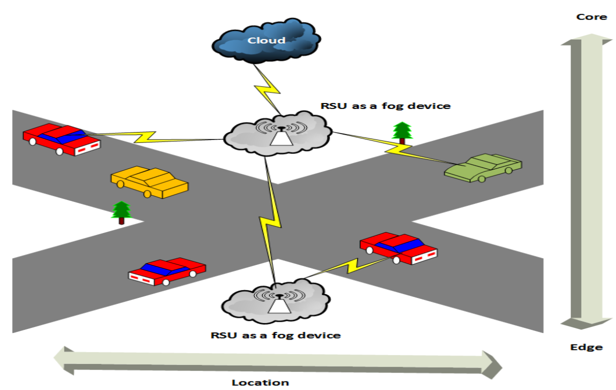


Fig. 3. Fog based architecture

In reality, as a result of privacy sensitivity of road event information as well as unauthentic interconnection of mobile sensors and the corresponding road infrastructure, inclusive of the RSUs such transmissions experience major challenges. A number of issues that need to be addressed in design of the security protocol includes a guarantee that the road event is not accessed at the time of transmission by unauthenticated users as well as consideration for its scalability. It is supposed that the generated data remain encrypted and hence the system should not only be able to just verify but also to simultaneously decrypt the data based on low computational and communication costs. Additionally, the protocol should attain mutual authentication among sensors, RSU gadgets as well as the cloud servers. Further, the protocol should be lightweight as a result of constraints in energy use and storage. Also, the protocol needs to retain its robustness when there is

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.2017.2666783, IEEE Internet of Things Journal

a threat; for instance, a case where the authentication keys remain exposed.

In order to successfully address the aforementioned issues, certificateless public key cryptography (CLPKC) [16] is used in pursuing the security objectives. CLPKC avoids often experienced key escrow problem that is associated with identity-based public key cryptography, commonly abbreviated as IDBC. As the user's private keys in CLPKC are not only offered by the Key Generator Center (KGC) but a combination of KGC's and the user's partial private keys. Nonetheless, the KGC lacks information of the user's full private key. Furthermore, CLPKC successfully evades the certificates management with regard to certificate-based public key cryptography like revoking, distributing and storing data. In order to achieve efficiency in terms of computational cost and communication overhead, we adopt signcryption technique to accomplish both encryption and signature in one logical step.

In order to adjust current work by adopting signcryption technique, certificateless schemes of signcryption (CLSC) are used in capturing communication with respect to both confidentiality and unforgeability. The first scheme of CLSC was proposed by Barbosa and Farshim [11] using a formal security analysis as evident in random oracle model. The CLSC protocol is premised on the process of aggregation that lowers the volume of exchanged information, signature verification as well as massive data unsigncryption thus attaining scalability, and lower computational and communication costs. These can be achieved with a single step and is of particular importance to low communication network bandwidths as well as computationally restricted environments. Eslami et al. and Lu et al. proposed certificateless aggregate signcryption scheme (CLASC) [12], [13]. However, these schemes are realized using many pairing operations that may lead to high computational cost and time consumption if there is an increase in the number of mobile sensors. Motivated by the above mentioned issues, our contributions are twofold:

- We propose a new efficient certificateless aggregate signcryption scheme CLASC with a significant improvement over pairings required by existing aggregate signatures verifications and unsigncryption. Our CLASC scheme has the lowest computational cost compared to the existing schemes [12], [13].
- Based on our proposed CLASC scheme, we design a privacy-preserving protocol, for enhancing security in data transmission of vehicular crowdsensing based road surface condition monitoring system using fog computing. The proposed protocol achieves data confidentiality, integrity, mutual authentication, privacy and anonymity through utilizing proposed CLASC scheme.

The remainder of the paper is organized as follows. In section II, we summarize road surface condition monitoring systems and certificateless aggregate signcryption related work. The system goals and security objectives are presented in section III, followed by the preliminaries in section IV. In section V, the CLASC scheme is presented in detail. Section VI describes the proposed privacy-preserving protocol and security analysis is given in section VII, followed by performance analysis in section VIII. We conclude our work in section IX.

II. Background and Related Work

This section begins by providing an overview of fog networking architecture and then investigating some of the existing systems for road surface condition monitoring before presenting a privacy-preserving protocol that uses certificateless aggregate signcryption scheme.

A. Fog networking architecture

Fog networking is a new architecture that provides storage, communications, control, configuration, measurement and management between terminal devices and the Internet with significant features, including location awareness, geographic distribution and low response latency [4], [5]. In the fog networking, a huge number of decentralized mobile devices can self-organize to communicate and potentially collaborate with each other via a fog node located at the edge of the Internet. There are several dimensions in fog architecture in term of the current standard practice [35]. At or near the end-user, essential amount of storage is carried out rather than storing in large-scale data centers. Moreover, instead of all routed through the backbone network, fog performs a substantial amount of communication at or near the end-user. Furthermore, a fundamental amount of management, including network measurement, control and configuration, at or near the end-user is carried out. Each node in the fog networking must be able to act as a router for its neighbors and be flexible to node mobility. As a special instantiation of mobile ad-hoc networks (MANETs), crowd sensing vehicular networks (CSVN) is applying the principles of MANETs that could be the basis for future fog networks [34]. Without requiring fixed and costly infrastructures to be available beforehand, MANETs will enable the formation of densely populated networks. More precisely, data collected by sensors are sent to devices like network edge, routers, access point for processing, not sent to cloud server thus fog computing paradigm reduces the traffic due to low bandwidth. Also, Fog computing improves the quality of service and minimizes latency. Therefore, Fog computing plays an important role by reducing the traffic of data to the cloud and not delaying the computation and communication due to placing near to the data sources.

B. Road surface condition monitoring system

Modern devices especially mobile devices have made sensing capabilities possible through the use of multiple powerful embedded sensors including accelerometers, gyroscopes and GPS systems, among others. We thus evaluate multiple scenarios/applications where mobile sensors are used in detection and reporting road surface conditions. Eriksson et al. proposed Pothole Patrol (P2) [2], a mobile sensing app used in detection and reporting of road surface condition. In this system, they used a taxi cabinet in which multiple accelerometer sensors were placed and used in the collection of multiple predefined patterns associated with road surface anomalies via manual labelling. In the experiment, Eriksson et al. equipped taxis with an embedded Linux computer system and were able to detect more than 90% of potholes. In a similar system used in traffic sensing and communication, Mohan et al. [14] proposed the use of mobile devices hooked up to integrated

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.2017.2666783, IEEE Internet of Things Journal

sensors to the exterior. Further, Mednis et al. [15] improved on the Pothole Patrol (P2) system using a customized embedded gadget and extended the approach using vehicular sensor networks operated using wireless sensor networks with the help of smartphones hardware platform for sensing road surface conditions [3]. The framework used involved synchronization and linkage of the data collection system with a database server for storage. A majority of such applications use cloud based architecture. However, in this paper, the system proposed is a privacy-preserving protocol that uses fog architecture.

C. Certificateless Aggregate signcryption scheme

The proposed protocol is based on privacy preservation using an aggregate scheme of signcryption that is certificate-less. Hence the focus of this work will be on existing certificateless aggregate signcryption scheme (CLASC) literature. Certificateless public key cryptography was first proposed by Al-Ryiami and Paterson [16] as a way of overcoming the challenges associated with key escrow as applied in cryptography approaches that are identity-based and hence maintain certificate freeness. There are several schemes proposed in encryption [17], [18], digital signature [19], [20], and signcryption [11], [21], [22], [23], certificateless cryptography. Since we are using certificateless aggregate signcryption, we evaluate multiple aggregate signcryption as used in identity based aggregate schemes of signcryption [24], [25]. Certificateless aggregate signcryption scheme (CLASC) is emphasized [13] as an appropriate secure model as has been proven in its use in the random oracle model [26]. Further, Eslami and Pakniat [12] argued in favour of certificateless aggregate signcryption scheme as a secure system. Nonetheless, the scheme as currently constituted requires significant improvements over pairing maps that can potentially lead to a promising low computational scheme in addition to lowering time consumption. We propose a new and efficient certificateless aggregate signcryption (CLASC) scheme by building on the random oracle model.

III. System models and design goals

This section describes our system model, attack model and design goals.

A. System model

Motivated by the various applications found in current literature, we consider that the road surface condition monitoring system comprises of a control center (CC), mobile sensors, e.g., vehicles and smart devices, roadside units (RSUs) as a fog device, and cloud servers, as shown in Fig. 4.

- Control center (CC) is a trustable entity in charge of the entire system and responsible for initializing the system. In the proposed scheme, CC works as the key generation center. CC only generates partial private key for the registers to avoid the key escrow problem and is blocked to access the sensors and RSUs sensitive data. It is assumed that the CC is powered with sufficient computation and storage capabilities.
- Mobile sensors, which may be embedded to vehicles and smart devices, generate a bunch of data, such as time, location and the actions signals, during road events, i.e., pothole or accidents.
- Roadside unit (RSU) is considered as an efficient computational and storage device that can extend the cloud services to the edge. RSUs have the ability to react and make decisions close to the end users. All the real time data sensed by the mobile sensors are sent to the RSU for immediate processing. Once processed, the RSUs can send for example an alert regarding road hazards at a specific location.
- Cloud servers are the data centers of the system. The system data such as historic information are stored in the cloud to be utilized later. The advantage of a fog device is that instead of sending all the data generated by the sensors to the cloud for processing (which can lead to high bandwidth cost and high latency), RSUs do the computation at the edge and only send the results to the cloud and the connected devices.

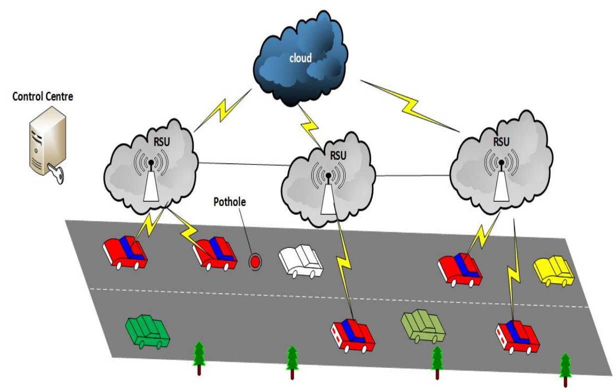


Fig. 4. System model

B. Attack model

In this study, we assume that the connection between RSUs and cloud is secure. We focus our attention to the threat to data generated by the sensors which is then forwarded to the RSUs. Road event reports devoid of content oriented privacy may result in eavesdroppers disclosing the road event report of the source and make the receiver get false road event reports. Malicious attackers may modify or fabricate the data for their own purposes. **particularly, the adversary can control the whole communication channel and monitor all the data pass through the channel. The adversary can also tamper the message, drop some packets and even replace the original message. Furthermore, the adversary can also capture and compromise a small number of RSUs and mobile sensors. All the data transmitted to/through compromised RSUs and mobile sensors can be intercepted and analyzed by the adversary. Moreover, we also take into account the scenario where some RSUs become malicious and can transmit forged reports to vehicles to make them react in a certain way. At the same time, a vehicle or a drive could become malicious by generating false reports for his own benefits, for example, gaining credits for contributing to a crowdsensing task. Ultimately, the third trust party that is the CC in this application scenario may disclose users authentication keys and fabricate the road event reports.**

C. Design goals

In this paper, we aim to achieve the following security and performance objectives based on the system model and potential threats.

1) Security objectives
   - *Data confidentiality and integrity.* All accepted messages should be delivered unaltered, and the origin of the messages should be protected i.e., from revealing private and sensitive information.
   - *Mutual authentication.* The mobile sensors and the RSU should authenticate each other in order to guarantee that the data from the source and once received is unaltered.
   - *Anonymity.* The identities of mobile sensors should be hidden from a normal message receiver during the authentication process to protect the sender's private information.
   - *Key escrow resilience.* The key generation center doesn't have the users full private keys. Therefore, we ensure that the adversary cannot get user's full private keys if KGC is compromised.
2) Performance objectives
   - *Low communication overhead and fast verification.* The security scheme should be efficient in terms of communication overhead and acceptable processing latency. A large number of report signatures should be first verified and then unsigncrpted in a short interval.
   - *Robustness.* The data generated via mobile sensors should not be accessed in case part of the private keys is infiltrated.
   - *Light weight.* Mobile sensors and devices have constraints such as limited power and storage. Therefore the proposed scheme should have low computational cost.

IV. Preliminaries

This section starts with basic concepts and portrays the necessary complexity assumptions. Then, the framework and security model of certificateless aggregate signcryption scheme is presented.

A. Bilinear maps

In this section, we recall the bilinear pairing technique, which serves as the basis of our proposed certificateless aggregate signcryption scheme. Let G be an additive group of large prime order q, and G_T be a multiplicative group of the same large prime order and P be a generator of G. An admissible bilinear pairing $\hat{e} : G \times G \to G_T$ is a map with the following properties:

- Bilinearity: for all $P, Q \in G$ and $a, b \in Z_q^*$,we have $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{a_b}$
- Non-degeneracy: $\hat{e}(P,Q) \neq 1_{G_T}$ where 1_{G_T} denotes the identity element of group G.
- Computability: there exists an efficient algorithm to compute $\hat{e}(P,Q)$ for $P,Q \in G$. An admissible bilinear pairing $\hat{e} : G\times G \to G_T$ can be implemented by the modified Weil/Tate pairings over elliptic curves [29].

Definition 1: Bilinear Parameter Generator. A bilinear parameter generator Gen is a probabilistic algorithm that takes a security parameter k as input, and outputs a 5-tuple $(G, G_T, \hat{e}, P, q)$ where q is a k-bit prime number, G,G_T are two groups with order q, $P \in G$ is a generator, and $\hat{e}$ is a non-degenerated and efficiently computable bilinear map.

B. Complexity assumptions

We recall the following intractability assumptions related to the security of our scheme.

Definition 2: Computational Diffie-Hellman (CDH) problem assumption. The challenger chooses $a, b \in Z_q^*$ at random and given a generator P of an additive group G with order q and output (aP, bP). The CDH problem is to compute abP. An adversary $\mathcal{A}$, has a probability of at least ε in solving the CDH problem if $Pr\ [\mathcal{A}\ (P, aP, bP) = abP] \geq \varepsilon$. The CDH assumption holds if the advantage of any probabilistic polynomial time PPT adversary $\mathcal{A}$ is negligible in solving the CDH problem.

Definition 3: Decisional Bilinear Diffie-Hellman (DBDH) problem assumptions. Given a generator P of an additive group G with order q, the challenger randomly chooses $a, b, c, x \in Z_q^*$ and (aP, bP, cP, x), then the BDH problem is to determine the value of x either equals to $\hat{e}(P,P)^{abc}$ or not.

C. Framework of certificateless aggregate signcryption

Based on Eslami et al. [12] and Lu et al. [13], we first define the participants involved in a framework of a certificateless aggregate signcryption scheme. They are composed of four parties which are: a key generator center KGC, an aggregating set ID_i of n users with an identity $\{ID_i\}_{i=1}^n$, a receiver with an identity ID_R and an aggregate signcryption generator. The framework of a certificateless aggregate signcryption scheme is defined by the following seven PPT algorithms:

- Setup: This algorithm takes a security parameter k as input and outputs system parameters $params$ and a master private key s, a corresponding master public key P_{pub}. Then, the KGC carries out the algorithm and publishes $params$. The key s is kept secure.
- Partial-Private-Key-Extract: Given the system parameters $params$, s and identity ID_i of an entity i. It returns a partial private key D_i. Then, the KGC calculates the algorithm to generate D_i that is sent to the corresponding user i through a secure channel.
- User-Key-Generate: This algorithm is run by each user and takes $params$ and user's identity ID_i as input. It returns a randomly chosen secret value x_i and a corresponding public key Y_i for the entity. Then, the user generates his own public key and publishes his public key.
- Signcrypt: This algorithm runs by each user ID_i in an aggregating set of n users $\{ID_i\}_{i=1}^n$. It takes $params$, some state information Δ. All of the users must use

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.2017.2666783, IEEE Internet of Things Journal

the same unique state information in the signcryption algorithm for an aggregating set, a message M_i, users identity ID_i with corresponding public key Y_i and private key (x_i, D_i), the receiver identity ID_R with corresponding public key Y_R as input. This algorithm returns a ciphertext C_i.

- Aggregate: This algorithm is run by the aggregate signcryption generator and takes an aggregating set ID_i of n users $\{ID_i\}_{i=1}^n$, Δ, users identity ID_i of each sender with corresponding public key Y_i and C_i on a message M_i as input. The message is ciphered with the state information Δ with the receiver identity ID_R with corresponding public key Y_R. It outputs an aggregated ciphertext C on messages $\{M_i\}_{i=1}^n$.
- Aggregate-Verify: This algorithm is performed by the the receiver ID_R and takes as input an aggregating set of n users $\{ID_i\}_{i=1}^n$, user's identity ID_i of each sender with corresponding public key Y_i, the receiver identity ID_f with corresponding public key Y_R , state information Δ, and an aggregated ciphertext C. If the aggregate signcryption is valid, algorithm returns true otherwise false.
- Aggregate-Unsigncrypt: The receiver ID_R performs this algorithm that takes as input an aggregated ciphertext C, state information Δ, the receiver full private key (x_R, D_R), his identity ID_f and public key Y_R, and the senders identities $\{ID_i\}_{i=1}^n$ with their corresponding public keys $\{Y_i\}_{i=1}^n$. It returns a set of n plaintexts $\{M_i\}_{i=1}^n$.

D. Security model of CLASC

A certificateless cryptography may be subject to two types of adversary [16]. Type I adversary may request entities public keys and replace keys with values of its choice but is not allowed to access the master private key. Type II adversary on the other hand may access the master private key but is not allowed to replace the public key of the entities. The CLASC scheme has two security objectives which are: confidentiality for the signcryption and encryption mode. And unforgeability for signcryption and signature mode. There exists an interactive game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ to prove the security of a CLASC scheme. There are four games for confidentiality and unforgeability between $\mathcal{C}$ and type I, type II adversary respectively. Eslami et al. [12] provide details for the four games and we refer to their work for the security model of a CLASC scheme and also, provide the definitions based on the games as declared in their work.

Definition 4: Confidentiality of CLASC. A CLASC scheme is semantically secure under adaptively chosen ciphertext attacks (IND-CCA2) if no PPT adversary (of either Type) has a non-negligible advantage in Game I or Game II. As the adversaries can access the private keys of all of the senders, therefore; this definition assures that confidentiality is preserved even if these keys are compromised and insider security is guaranteed.

Definition 5: Unforgeability of CLASC. A CLASC scheme is existentially unforgeable under adaptively chosen message attacks (EUF-CMA) if no PPT adversary (of either Type) has a non-negligible advantage in the Game III or the Game IV. As the adversaries can access the private key of the receiver, therefore this definition assures that unforgeability is preserved even if this key is compromised and insider security is guaranteed.

V. PROPOSED CLASC

In this section, we propose an efficient CLASC scheme that serves as the design basis for our privacy-preserving protocol.

We propose a solid CLASC scheme based on the schemes of Eslami et al. [12] and Lu et al. [13]. They utilize the bilinear map that is an efficient way of pairing. However, their schemes may suffer from high computational complexity because of the number of pairing operations for signcryption, aggregate, aggregate verification and aggregate unsigncryption. Therefore, we address this problem by reducing pairing operations that provide low computational and communication cost. The proposed CLASC scheme is composed by the following six algorithms.

- **Setup**: Given the security parameters k, and this algorithm is performed by the KGC as follows:
  - Chooses a cyclic additive group G of prime order q on elliptic curve, and P is an arbitrary generator of G.
  - Chooses a cyclic multiplicative group G_T of the same order q and a bilinear map $\hat{e} : G \times G \rightarrow G_T$.
  - Randomly selects a master private key $s \in Z_q^*$ and compute the master public key $P_{pub} = sP$.
  - Selects four secure hash functions H_1 :$\{0,1\}^* \rightarrow Z_q^*$, H_2 :$\{0,1\}^* \rightarrow \{0,1\}^n$ here n is the bit-length of plaintexts, H_3: $\{0,1\}^* \rightarrow G$ and H_4: $Z_q^* \rightarrow G$.
  - Publishes the system parameter $params = (G, G_T, \hat{e}, P, q, P_{pub}, H_1, H_2, H_3, H_4)$ and the master private key s will be kept secure by the KGC.
- **Key-Generation**: This algorithm is interactively performed by the user ID_i and KGC as follows:
  - The user ID_i randomly chooses $x_i \in Z_q^*$ as the secret value and computes a partial public key $Y_{ib} = x_i P$.
  - The user sends its identity and partial public key (ID_i, Y_{ib}) to the KGC.
  - The KGC then randomly selects $y_i \in Z_q^*$ and compute another partial public key for the user $Y_{ia} = y_i P$, so the full public key for the user is (Y_{ib}, Y_{ia}).
  - The KGC computes the partial private key $D_i = y_i + s * Q_i$ where $Q_i = H_1(ID_i)$,and D_i is sent securely to the user ID_i.
  - The user ID_i judges the validity of the partial private key by checking $D_i P = Y_{ia} + P_{pub} H_1(ID_i)$.

  Notably, these procedures finish three different algorithms which are, *set-secret-value*, *partial-private-key-extract* and *set-public-key* of the proposed scheme. These algorithms generate public key (Y_{ib}, Y_{ia}) that is kept in the public tree by the KGC, and the full private key (x_i, D_i) is kept secret by the user.

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.2017.2666783, IEEE Internet of Things Journal

- **Signcrypt**: This algorithm is performed by a sender ID_i to signcrypt the message m_i with ID_R as a receiver. ID_i performs the algorithm as follows:
  - ID_i randomly selects $r \in Z_q^*$ and compute $T_i = rP$,
  - Compute $Z_b = rY_{rb}$,
  - Compute $Z_a = r(Y_{ra} + P_{pub}Q_i)$,
  - Compute $h_a = H_2(ID_R||Y_{ra}||Y_{rb}||\Delta||T_i||Z_b||Z_a)$,
  - Compute $K_i = h_a \oplus m_i$, and compute
  - $h_b = H_3(ID_R||Y_{ra}||Y_{rb}||\Delta||T_i||K_i||Q_i||Y_{ib}||Y_{ia})$,
  - Compute $h_c = H_4(\Delta)$,
  - Compute $\alpha_i = D_i h_c + r h_b + x_i h_c$.
  - Return the ciphertext $C_i = (T_i, K_i, \alpha_i)$
- **Aggregate:** This algorithm is performed by aggregator signcryption generator on the receiver ID_R as follows:
  - Compute $\alpha = \sum_{i=1}^{n} \alpha_i$
  - This algorithm outputs the aggregate ciphertexts $C = (T_1 ... T_n, K_1 ... K_n, \alpha)$
- **Aggregate-Verify:** This algorithm is run by a receiver ID_R and computes the following:
  - $h_b = H_3(ID_R||Y_{ra}||Y_{rb}||\Delta||T_i||K_i||Q_i||Y_{ib}||Y_{ia})$, for $i = 1 ..., n$,
  - $h_c = H_4(\Delta)$,
  - Verify $\hat{e}(\alpha, P) =$
  $\hat{e}(\sum_{i=1}^{n} Y_{ia} + P_{pub}Q_i, h_c)\hat{e}(\sum_{i=1}^{n} T_i, h_b)\hat{e}(\sum_{i=1}^{n} Y_{ib}, h_c)$
  If the above equation holds, this algorithm outputs true otherwise false.
- **Aggregate-Unsigncrypt**: If the output of Aggregate-Verify algorithm is true, this algorithm is performed by the receiver ID_R as follows:
  - Compute $Z_b{}' = x_r T_i$,
  - Compute $Z_a{}' = D_r T_i$, and compute
  - $h_a{}' = H_2(ID_R||Y_{ra}||Y_{rb}||\Delta||T_i||Z_b{}'||Z_a{}')$,
  - Compute $m_i{}' = K_i \oplus h_a{}'$
  - This algorithm outputs $\{m_i\}_{i=1}^{n}$.

- Correctness of the signatures:

$$\hat{e}(\alpha, P) = \hat{e}(\sum_{i=1}^{n} \alpha_i, P)$$
$$= \hat{e}(\sum_{i=1}^{n} (D_i h_c + r h_b + x_i h_c), P)$$
$$= \hat{e}(\sum_{i=1}^{n} D_i h_c, P)\ \hat{e}(\sum_{i=1}^{n} rP, h_b)\ \hat{e}(\sum_{i=1}^{n} x_i P, h_c)$$
$$= \hat{e}(\sum_{i=1}^{n} D_i P, h_c)\ \hat{e}(\sum_{i=1}^{n} T_i, h_b)\ \hat{e}(\sum_{i=1}^{n} Y_{ib}, h_c)$$
$$= \hat{e}(\sum_{i=1}^{n} (Y_{ia} + P_{pub}Q_i, h_c)\hat{e}(\sum_{i=1}^{n} T_i, h_b)\hat{e}(\sum_{i=1}^{n} Y_{ib}, h_c)$$

- Correctness of the decryption
  $m_i{}' = K_i \oplus h_a{}'$
  = $H_2(Q_i||Y_{ia}||Y_{ib}||\Delta||T_i||Z_b||Z_a) \oplus m_i \oplus h_a{}'$
  = $h_a \oplus m_i \oplus h_a{}'$
  = m_i

VI. Proposed privacy-preserving protocol

In this section, we present the details of our privacy-preserving protocol. In this application scenario, mobile sensors are considered as a fog device, which aggregates the data, aggregates verification and then aggregates unsigncryption. Our certificateless aggregate signcryption scheme is introduced in the protocol to fulfill the design objectives. The proposed protocol consists of four steps: system initialization, data formulation and sending, SRER aggregated verification, and data receiving.

A. System initialization

The mobile sensors and RSUs register to the CC to generate their full private keys and public keys. Moreover, it determines the format of road event report that is generated by the mobile sensors. Furthermore, routing is also established in this part.

Given the security parameter k, the CC first generates the bilinear parameters $(G, G_T, \hat{e}, P, q)$ by running $Gen(k)$. Then, the CC selects a random $s \in Z_q^*$ as its master secret key and computes its master public key $P_{pub} = sP$. Additionally, the CC chooses four secure hash functions: H_1 :$\{0,1\}^* \rightarrow Z_q^*$, H_2 :$\{0,1\}^* \rightarrow \{0,1\}^n$ here n is the bit-length of plaintexts, H_3: $\{0,1\}^* \rightarrow G$ and H_4: $Z_q^* \rightarrow G$. After that, the system parameters $params$ will be published, which include $(G, G_T, \hat{e}, P, q, P_{pub}, H_1, H_2, H_3, H_4)$.

A significant task of the setup procedure is to determine the format of secure road event report $SRER_{ij}$. For a road event RE_i , the mobile sensors Sen_j will generate the data where $Data_i = (Time_{ij}, Location_i, Signals_i)$ and the $SRER_{ij}$ will securely forward to the RSU in the format $SRER_{ij} = (Q_j, Signcrypt(Data_i))$ where,
$Time_{ij}$ - denotes the time when the vehicle j makes the claim on this emergency event i.
$Location_i$ - denotes the place where the road event takes place.
Q_j - denotes the pseudo identity of the mobile sensor that generates the claim.
$Data_i$ - denotes a report generated by a mobile sensor about road event.
$Signcrypt_ij$ - denotes the signcryption generated by the sensor Sen_j on the road event RE_i that sends to RSU.

Mobile sensors and RSUs can join the system by performing the following Steps:

- A mobile sensor Sen_j can randomly choose $x_j \in Z_q^*$ as its secret value and compute its partial public key $Sen_{jb} = x_j P$. To keep the identity privacy, the Sen_j can also randomly choose Q_j as its pseudo identity.
- Sen_j sends its identity and partial public key (Sen_j, Sen_{jb}) to the CC for registration.
- The CC randomly selects $y_j \in Z_q^*$ and compute another partial public key for the mobile sensor $Sen_{ja} = y_j P$.
- The CC then computes the partial private key $D_j = y_j + s * Q_j$,where $Q_j = H_1(Sen_j)$, for the register Sen_j with partial public key Sen_{jb}.
- D_j is sent to the Sen_j via a secure channel. The full public key (Sen_{jb}, Sen_{ja}) is kept in the public tree by the CC.
- mobile sensor Sen_j receives the partial private key D_j and concatenates with its secret value x_j to form

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.2017.2666783, IEEE Internet of Things Journal

its full private key (D_j, x_j)

The user Sen_j judges the validity of the partial private key by checking $D_jP = Sen_{ja} + P_{pub}H_1(Sen_j)$.

B. Data formulation and sending

This part is performed by the source with a mobile sensor Q_j. A road event RE_i is sensed by one or multiple mobile sensors and then $Data_i$, which include $(Time_{ij}, Location_i, Signals_i)$, is discovered. After that, Q_j with encrypted $Data_i$ as a $SRER_{ij}$ sends to the RSU as fog device receiver. Then, Q_j utilizes the certificateless signcryption algorithm on $Data_i$ as follows:

- Sen_j randomly selects $r \in Z_q^*$ and compute $T_j = rP$,
- Compute $Z_b = rPK_{rb}$,
- Compute $Z_a = r(PK_{ra} + P_{pub}Q_j)$,
- Compute $h_a = H_2(ID_R||Pk_{ra}||PK_{rb}||\Delta||T_j||Z_b||Z_a)$,
- Compute $K_j = h_a \oplus Data_i$ and compute,
- $h_b = H_3(ID_R||Y_{ra}||Y_{rb}||\Delta||T_j||K_j||Q_j||Sen_{ja}||Sen_{jb})$
- Compute $h_c = H_4(\Delta)$,
- Compute $\alpha_j = D_jh_c + rh_b + x_jh_c$.

The ciphertext $C_j = (T_j, K_j, \alpha_j)$ is attached to secure road event report in the format as $SRER_{ij} = (Q_j, Signcrypt(Data_i)$, where $Signcrypt(Data_i) = C_j$.

It is worth pointing out that using only pseudo identities in vehicular networks to preserve driver privacy is insufficient [31].This is because due to the nature and characteristics of vehicular networks, vehicle mobility can be predicted. As a result, even the vehicle's pseudo identities change, the reported locations in the future traffic information from a vehicle can be used to link pseudo identities and even worse a real-world identity could be discovered. In order to address the problem, several mechanisms have been proposed in the past. For example, using silent period [31], creating mix-zones [32]. In our proposed scheme, we can adopt the mix-zone technique. For instance, when all the vehicles approaching an intersection where there is an RSU deployed, they coordinate with each other and change their pseudo identities at the same time. Also, their public and private keys are updated accordingly with the involvement of CC through the RSU. CC will update the public tree with the vehicles new public keys as well.

C. SRER aggregated verification

Notably, this application scenario is based on Vehicles to Infrastructure communication (V2I) which means mobile sensors can directly communicate with the RSUs. Once a road event RE_i is sensed by one or multiple mobile sensors, they then generate a road event report $SRER_{ij}$ that includes accurate information such as time, location and the type of event. We utilize this system on the highway, that massive of objects can pass through. Therefore, a bunch of data will be generated by the various mobile sensors and sent to the closest RSU. If the RSU receives each ciphertext separately to verify the signature and then usingcrypt it, this process will have a long time that may lead to long delay. We exploit an advantage of fog devices, which are efficient in computational cost and bandwidth. Therefore, our protocol provides the aggregation property that the RSUs can aggregate all the ciphertexts generated by the multiple mobile sensors.This process provides a sufficient amount of efficiency over sending each ciphertext separately. Whenever receiving a SRER, the aggregator will perform the SRER aggregation and SRER batch verification operations as follows.

1) SRER aggregation: Aggregate SRER is used to aggregate multiple SRERs into a single SRER. For a road event RE_i , given n SRERs $SRER_{ij}$ = $(Q_j, Signcrypt(Data_i))$ by mobile sensors $Sen_1, ...Sen_n$, we can obtain $SRER_{agg}$ = $(Q_1...Q_n, Signcrypt(Data_i)_1^i ... Signcrypt(Data_i)_i^n)$. This algorithm is performed by an aggregate signcryption generator on the receiver as follows:

- This algorithm takes a collection of individual ciphertexts $C_j = (T_j, K_j, \alpha_j)_{j=1}^n$ generated by mobile sensors with $(Q_j)_{j=1}^n$ to a receiver with identity ID_R under the same state information Δ, which is considered as a secret value to insure the aggregation phase.
- We have aggregated the signature parts of ciphertexts and, an aggregate signcryption generator computes the signature aggregation $sig_{agg} = \sum_{j=1}^{n} \alpha_j$.
- It outputs the aggregate ciphertexts $SRER_{agg} = ((Q_j)_{j=1}^n, T_1...T_n, K_1...K_n, sig_{agg})$.

2) SRER batch verification: This step performs signature batch verification for all the ciphertexts simultaneously. Given the signature aggregation sig_{agg}, the report sets $SRER_{ij}|\leq i \leq n$, corresponding public keys $(Sen_{ja}, Sen_{jb})|\leq i \leq n$ for all the mobile sensors and a receiver's identity ID_R, and its corresponding public key (Pk_{ra}, PK_{rb}) using the same state information Δ.

In summary, the tuples given are $(SRER_{agg}, (Q_j)_{i=1}^n, (Sen_{ja},, Sen_{jb})_{j=1}^n, ID_R,$ $(Pk_{ra}, PK_{rb}), x_R, D_R, \Delta)$. In order to verify the signature, this algorithm computes the following:

- $h_b = H_3(ID_R||Y_{ra}||Y_{rb}||\Delta||T_i||K_i||Q_i||Sen_{ja}$ $||Sen_{jb})$, for $j = 1, ..., n$
- $h_c = H_4(\Delta)$,

The signature aggregation Sig_{agg} accept if

$$\hat{e}(sig_{agg}, P) =$$
$$\hat{e}(\sum_{i=1}^{n}(sen_{ja} + P_{pub}Q_j, h_c)\prod_{i=1}^{\infty}\hat{e}(\sum_{i=1}^{n}T_i, h_b)\hat{e}(\sum_{i=1}^{n}sen_{jb}, h_c)$$

If the batch verification holds, the aggregator will accept SRERs in list V as a valid SRERs. Then the aggregated SRER $SRER_{agg}$ in V will be forwarded to complete unsigncryption step. Once a road event report SRER is verified valid, RSU pursues the next unsigncryption step.

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.2017.2666783, IEEE Internet of Things Journal

D. Data receiving

The RSUs decrypt the SRERs when the signature verification outputs true. The RSU continues to complete the decryption phase as follows:

- $Z_b{}' = x_r T_j$, $Z_a{}' = D_r T_j$
- $h_a{}' = H_2(ID_R||Pk_{ra}||PK_{rb}||\Delta||T_j||Z_b{}'||Z_a{}')$,
- $Data_i{}' = K_j \oplus h_a{}'$

VII. Security Analysis

In this section, the security of the proposed protocol has been analyzed according to the security objectives described in Section III.

The proposed protocol achieves road report $Data_i$ confidentiality and integrity. The mobile sensor signcrypts $Data_i$ as $C_j = (T_j, K_j, \alpha_j)$, where T_j and K_j fulfill the encryption part and α_j achieves digital signature in one logical step. Only the RSU unsigncrypts $Data_i{}'$ by computing T_j, K_j and α_j. Therefore, according to *Definition 4* and *Definition 5* the encryption and signature achieve confidentiality and Unforgeability under CDH problem.

The protocol can achieve the mutual authentication. RSU is authenticated by the signcryption on the road report $Data_i$ that generated by the mobile sensor. Particularly, In the proposed scheme, in order to restore the source identity of the road report and unsigncrypt it, only the RSU that holds the private key $(D_R, x_R)$is able to perform these procedures. The mobile sensor computes Z_a and Z_b through the signcryption algorithm to establish the mutual authentication. RSU authenticates the source road report by verifying the signcryption on the $Data_i$. Therefore, according to *Definition 5* we deduce that the adversary cannot forge the signature on the message without the full private key under DBDH problem in the signcryption unforgeability theorem.

The proposed protocol achieves anonymity. The mobile sensor uses its pseudo identity Q_j , that is generated from its real identity during the entire road report transmission processes, for anonymity. Anyone (including the CC) cannot reveal the real identity of the requesting mobile sensor.

The proposed protocol achieves key escrow resilience because it relies on certificateless public key cryptography (CLPKC). The control center CC can only generate the partial private key for the user who is able to compute the full private key (D_j, x_j) after selecting its secret value x_j. Therefore, even the CC is compromised, we insure that the adversary cannot get user's full private keys.

VIII. Performance Analysis

In this section, we evaluate the performance of the proposed privacy-preserving protocol in terms of the computational cost and communication overhead. To demonstrate the efficiencies of proposed protocol, we compare proposed CLASC scheme with the existing schemes [12], [13], which suffer from computational complexity and communication cost due to the fact that pairing and exponentiation operations take much more computation time.

A. Computational cost

To the best of our knowledge, we compare the efficiency of our scheme with the certificateless aggregate signcryption scheme available in Eslami et al [12] and Lu et al [13]. As the operations scalar multiplication in G, exponentiation in G_T, and pairing dominate the computational cost, we consider those three operations in computing the time consumption. We denote t_p the time consumption of pairing, t_m the time consumption of a scalar point multiplication in G and t_e the time consumption of an exponentiation in G_T.

The proposed CLASC scheme, each sender signcrypts the data separately unlike the receiver that is able to aggregate verify all the signature parts of ciphertexts and then aggregate unsigncrypt. The signcryption algorithm takes six multiplication operations in G to compute both signature and encryption. On the other hand, the unsigncrypt algorithm needs four pairing operations and two scalar multiplication operations to aggregate verify the signature and unsigncrypt the ciphertexts.

On the receiver side, verification of signatures can be performed in a single step rather than verifying each signature separately. The computational cost in the receiver side is more efficient than existing schemes. Therefore, efficiency of aggregate sincryption schemes can be evaluated include t_p , t_m and t_e. The comparison of the computational cost among schemes are demonstrated in Table I.

TABLE I. Cryptographic Operations comparison with other CLASC schemes

Signcrypt			
schemes	t_p	t_m	t_e
Lu et.al	1	5	0
Ziba et.al	1	4	1
Proposed	0	6	0
UnSigncrypt			
schemes	t_p	t_m	t_e
Lu et.al	10	2	0
Ziba et.al	5	1	0
Proposed	4	2	0

While the proposed CLASC in table I is implemented without exponentiations, we demonstrate that the existing CLASC schemes have three operations on pairing, multiplication and exponentiation.

In order to evaluate the computation of efficiency of the proposed protocol, an MNT curve [27] with the Tate pairing $\hat{e}$: G $\times$ G $\rightarrow G_T$ defined over this curve will be employed, where the embedding degree of the curve is 6 and q is a 160-bit. The implementation was executed on an Intel Pentium IV 3.0 GHZ machine [28]. The running time is shown in table II.

TABLE II. Cryptographic Operations Running Time

Operation	Running Time	Descriptions
t_m	0.6 ms	The time for a scalar point multiplication
t_p	4.5 ms	The time for one pairing operation

Fig. 5 shows the comparison of computational cost between the existing CLASC schemes and our proposed scheme. It demonstrates that our proposed CLASC scheme needs much fewer computation of time than other CLASC schemes because of the fact that the pairing and exponentiation operations take

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.2017.2666783, IEEE Internet of Things Journal

much longer computation time than the multiplication operation. Our proposed scheme needs four **pairing operations** while the scheme in [12] has six **pairing operations** with one exponentiation operations and [13] has eleven **pairing operations**. Therefore, our proposed CLASC scheme is considered as a lightweight scheme because it has fewer number of pairing operations and does not perform exponentiation operations. Based on the running time results in [28], the computational cost in the whole scheme T_k $=8t_m$ + $4t_p$ = 8 * 0.6 + 4 * 4.5 = 22.8 ms. However, we have constraint devices of mobile sensors that act as a sender. Consequently, our scheme provide a lightweight signcryption that its time consumption $T_s = 6t_m$ = 3.6 ms. On the other hand, the receiver RSU, is a fog device that has a high computational capability and the time consumption for unsigncryption T_u $=2t_m$ + $4t_p$ = 19.2 ms, which is an efficient reasonable time assumption including aggregate ciphertexts , patch verification, and aggregate unsigncryption. From Fig. 5, we can observe that the computation cost of the CLASC scheme keeps constant even if the number of mobile sensors increases.

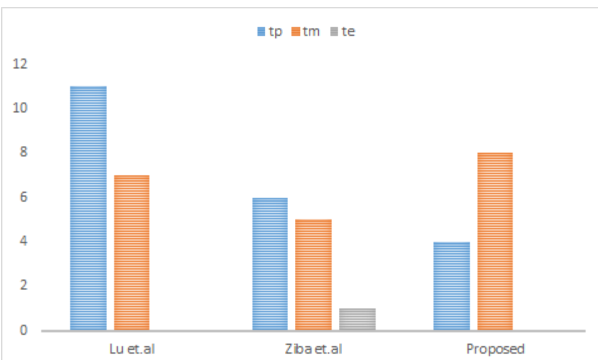


Fig. 5. Efficiency comparison with other CLASC schemes

B. Communication overhead

In the proposed CLASC scheme, the communication cost is determined by the size of the aggregated ciphertext length $SRER_{agg}$, which is mainly due to batch verification and aggregate unsigncryption. However, it is not possible to reduce the communication overhead of a CLASC scheme to a constant value because two parts of each ciphertext are needed for decryption. In contrast, the aggregated ciphertext $SRER_{agg}$ has $n + 1$ elements in G for achieving the security level. Therefore, we have an efficient protocol that has much fewer computational time than other schemes, without increasing the communication cost, as shown in table III. Thus, our proposed protocol is suitable for narrow bandwidth and terminals with limited resources.

TABLE III. COMPUTATIONAL AND COMMUNICATION OVERHEAD ANALYSIS

Scheme	Computational Overhead	Communication Overhead
Lu et.al	$11t_p + 7t_m$	$(n+1)\|G\|+n\|m\|$
Ziba et.al	$6t_p + 5t_m + t_e$	$(n+1)\|G\|+n\|m\|$
Proposed	$4t_p + 8t_m$	$(n+1)\|G\|+n\|m\|$

IX. CONCLUSIONS

In this paper, we propose a new efficient certificateless aggregate signcryption (CLASC) scheme. We then designed a privacy preserving vehicular crowdsensing road surface condition monitoring system using fog computing based on the proposed CLASC scheme. In addition, the proposed privacy-preserving protocol meets the security requirements such as data confidentiality and integrity, mutual authentication, anonymity and key escrow resilience. Extensive comparisons of computational cost and communication overhead show that the proposed scheme can achieve much better efficiency than the existing schemes.

REFERENCES

[1] M. Perttunen, O. Mazhelis, F. Cong, M. Kauppila, T. Leppanen, J. Kantola, J. Collin, S. Pirttikangas, J. Haverinen, T. Ristaniemi, and J. Riekki, ”Distributed road surface condition monitoring using mobile phones,” *Ubiquitous Intelligence and Computing*, Springer, pp. 6478, 2011.

[2] 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,” *Proc. 6th Int. Conf. Mobile Syst., Appl., Serv.*, pp. 29-39, 2008.

[3] G. Strazdins, A. Mednis, G. Kanonirs, R. Zviedris, and L. Selavo, ”Towards Vehicular Sensor Networks with Android Smartphones for Road Surface Monitoring,” *2nd International Workshop on Networks of Cooperating Objects (CONET’11), Electronic Proceedings of CPS Week’11*, 2011.

[4] I. Stojmenovic, ”Fog computing: A cloud to the ground support for smart things and machine-to-machine networks,” *Telecommunication Networks and Applications Conference (ATNAC), Australasian*, pp. 117-122, 2014.

[5] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, ”Fog Computing and Its Role in the Internet of Things,” *proceedings of ACM SIGCOMM*, Helsinki, pp. 13-16, 2012.

[6] M. Raya and J.-P. Hubaux, ”Securing Vehicular Ad Hoc Networks,” *J. Computer Security, Special Issue on Security, Ad Hoc and Sensor Networks,* vol. 15, no. 1, pp. 39-68, 2007.

[7] T. Little and A. Agarwal, ”An information propagation scheme for VANETs,” *IEEE Intell. Transportation Syst.*, pp. 155-160, 2005.

[8] C. Li, M. Hwang, and Y. Chung, ”A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks,” *Computer Communication*, vol. 31, pp. 2803-2814, 2008.

[9] 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*, Beijing, pp. 1451-1457, 2008.

[10] H. Zhu, X. Lin, R. Lu, P. H. Ho, and X. Shen, ”AEMA: An Aggregated Emergency Message Authentication Scheme for Enhancing the Security of Vehicular Ad Hoc Networks,” *2008 IEEE International Conference on Communications*, Beijing, pp. 1436-1440, 2008.

[11] M. Barbosa and P. Farshim, ”Certificateless signcryption,” Proceedings of the 2008 ACM symposium on Information, *computer and communications security*, pp. 369-372, 2008.

[12] Z. Eslami and N. Pakniat, ”Certificateless aggregate signcryption: Security model and a concrete construction secure in the random oracle model,” *Journal of Computer and Information Sciences*, vol. 26, no. 3, pp. 276-286, 2014.

[13] H. Lu, Q. Xie, ”An efficient certificateless aggregate signcryption scheme from pairings,” 2011 International Conference on Electronics, *Communications and Control (ICECC)*, pp. 132-135, 2011.

[14] P. Mohan, V. N. Padmanabhan and R. Ramjee, ”Nericell: rich monitoring of road and traffic conditions using mobile smartphones,” Proceedings of the 6th ACM conference on Embedded network sensor systems, *ser. SenSys ’08*, pp. 323-336, 2008.

[15] A. Mednis, A. Elsts and L. Selavo, "Embedded Solution for Road Condition Monitoring Using Vehicular Sensor Networks," Proc. 6th IEEE Int'l Conf, *Application of Information and Communication Technologies (AICT'12)*, pp. 1-5, 2012.

[16] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," *Proceedings of the Asiacrypt 2003*, LNCS, vol. 2894, pp. 452-473, 2003.

[17] S. Seo, M. Nabeel, X. Ding, and E. Bertino, "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds," IEEE Trans, *Knowledge and Data Engineering*, vol. 26, no. 9, pp. 2107-119, 2014.

[18] A. W. Dent, "A survey of certificateless encryption schemes and security models," *International Journal of Information Security*, vol. 7, pp. 349-377, 2008.

[19] B. Hu, D. Wong, Z. Zhang, and X. deng, "Certificateless signature: a new security model and an improved generic construction," *Designs, Codes Crypt*, Vol. 42, pp. 109-126, 2007.

[20] X. Huang, Y. Mu, W. Susilo, D. Wong, and W. Wu, "Certificateless signature revisited," *Proc. ACISP2007*, pp. 308-322, 2007.

[21] C. Wu and Z. Chen, "A new efficient certificateless signcryption scheme," International Symposium, *Information Science and Engieering*, ISISE'08., Vol. 1, pp.661-664, 2008.

[22] W. Xie and Z. Zhang, "Efficient and provably secure certificateless signcryption from bilinear maps," *Wireless Communications, Networking and Information Security (WCNIS)*, 2010 IEEE International Conference on, Beijing, China, pp. 558-562, 2010.

[23] F. Li , M. Shirase, and T. Takagi, "Certificateless Hybrid Signcryption," *The 5th Information Security Practice and Experience Conference (ISPEC 2009)*, LNCS 5451, Springer-Verlag, pp. 112-123, 2009.

[24] S.S.D. Selvi, S.S. Vivek, J. Shriram, S. Kalaivani and C.P. Rangan, "Identity based aggregate signeryption schemes," *Proceedings of Progress in Cryptology*, New Delhi, vol. 5922, pp. 378-397, 2009.

[25] J. Kar, "Provably secure identity-based aggregate signeryption scheme in random oracles," *IACR Cryptology ePrint Archive*, vol. 2013, pp. 37, 2013.

[26] M. Bellare and P. Rogaway, "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols," Proc. First ACM conference, *Computer and Communications Security*,(CCS ',93), pp. 62-73, 1993.

[27] A. Miyaji, M. Nakabayashi, and S. Takano, New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Transactions on Fundamentals*, Vol. E84-A, No. 5, pp. 1234-123, 2001.

[28] M. Scott, Efficient implementation of crytographic pairings, [Online]. Available: http://ecrypt-ss07.rhul.ac.uk/ Slides/Thursday/mscott-samos07.pdf

[29] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *Advances in Cryptology - CRYPTO*, vol. 2139, pp. 213-229, 2001.

[30] Ontario ministry of transportation, "Winter Driving - Be Prepared, Be Safe," Online http://www.theiet.org/resources/journals/research/

[31] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura and K. Sezaki, "CARAVAN: Providing location privacy for VANET," *Proc. of the Workshop on Embedded Security in Cars (ESCAR)*, pp. 1-15, 2005.

[32] J. Freudiger, M. Raya, M. Feleghhazi,P. Papadimitratos and J.P.Hubaux., "Mix Zones for Location Privacy in Vehicular Networks," *Proceedings of the First International Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS '07)*, Vancouver, British Columbia, Canada, 2007.

[33] N. Mitton, S. Papavassiliou, A. Puliafito and KS. Trivedi, "Combining Cloud and sensors in a smart city environment," *EURASIP journal on Wireless Communications and Networking*, pp. 1, 2012.

[34] L.M. Vaquero, and L. Rodero-merino, "Finding your way in the fog: Towards a comprehensive definition of fog computing," ACM SIGCOMM Comp. Commun. Rev., vol. 44, no. 5, pp. 2732, 2014.

[35] C. Mung, "Fog networking: An overview on research opportunities," Dec 2015, [online] Available: arxiv.org/pdf/1601.00835.pdf