Towards secure and privacy preserving collision avoidance system in 5G fog based Internet of Vehicles

Lewis Nkenyereye, Chi Harold Liu, JaeSeung Song

PII: S0167-739X(18)31758-8
DOI: https://doi.org/10.1016/j.future.2018.12.031
Reference: FUTURE 4652

To appear in: *Future Generation Computer Systems*

Received date : 26 July 2018
Revised date : 26 November 2018
Accepted date : 14 December 2018

Please cite this article as: L. Nkenyereye, C.H. Liu and J. Song, Towards secure and privacy preserving collision avoidance system in 5G fog based Internet of Vehicles, *Future Generation Computer Systems* (2019), https://doi.org/10.1016/j.future.2018.12.031

Towards Secure and Privacy Preserving Collision Avoidance System in 5G Fog based Internet of Vehicles

Lewis Nkenyereye[a], Chi Harold Liu[b], JaeSeung Song[a,*]

[a] *Sejong University, Seoul, Republic of Korea*
[b] *Beijing Institute of Technology, Beijing, China*

Abstract

Current avoidance systems mainly focus on the safety of the car occupants. The surrounding entities including the pedestrians, the cyclists are assumed to use a different avoidance system for their safety. Vehicle speed is reported as one of the major factors that causes such severe road accidents that affect other entities on the road. In response, several solutions have been implemented to control the causalities of over speeding ranging from speed camera, speed detectors to car avoidance systems. However, those solutions have not significantly improved the rate of traffic accidents and their impact. Additionally, the current solutions do not ensure timely notification of all the road users (surrounding vehicle drivers, pedestrians or others) that can alleviate crash causalities in case of fatal traffic accidents. The fifth generation (5G) cellular network is predicted to overcome the current limitations of Internet-of-Vehicles (IoV) by offering fast, low latency and reliable connections to enable IoV based applications. Fog computing has also been proposed to complement IoV by bringing computational entities in nearby proximity of the vehicles. 5G based fog vehicular networks is a new paradigm that empower real-time and low latency services for Intelligent Transportation System (ITS). In this paper we proposed a secure and privacy-preserving collision avoidance system in 5G fog based IoV. The fog devices are used to collect speed violation report (TVR) sent by the

[*] Corresponding author
Email address: jssong@sejong.ac.kr (JaeSeung Song)
URL: seslab.sejong.ac.kr (JaeSeung Song)

Preprint submitted to Future Generation Computer Systems *December 22, 2018*

vehicles' speed sensors. The fog nodes aggregate multiple TVRs, verify the signatures on the TVRs and broadcast anonymous notifications to other entities in the vicinity. The protocol makes use of certificateless aggregate signcryption coupled with pseudonymous technique as the building blocks to ensure authentication, integrity, confidentiality and privacy preservation respectively. The batch verification technique is used by the fog devices to allow simultaneous TVRs signature verification for a timely response. The authorization of reporting speed sensors is both guaranteed by the location-based information along with the digital signature to discard all the bogus TVRs. The analysis of the protocol confirms its lightweightness and efficiency.

Keywords: 5G cellular networks; fog computing; intelligent transportation system; security; collision avoidance system.

1. Introduction

The recent report of World Health Organization released in May 2017 records about 1.24 million people who die each year as a result of road traffic crashes. Road traffic injuries are cited to be the leading cause of death among young people, aged between 15 to 29 years and could be the seventh major cause of death by 2030 [1][2]. The same report ranges vehicle speed as of one of the main factors which cause road accidents along with the drink driving, non usage of belt and distractions. Approximately 90 % of the road accidents occur in low-and middle-income countries due to inadequate road safety infrastructure as well as poor traffic management system. In most high-income countries, around 20 % of all the traffic accidents are caused by exceeding the speed limit [3][4]. However, in these high income countries, most of the roads are equipped by cameras and speed detectors in order to monitor and latter on identify the drivers who violated the permitted speed limit. Though those cameras have significantly improved the traffic congestion issues, those infrastructures have not achieved significant result for preventing or alleviating the causalities caused by the traffic accidents [5][6]. Furthermore, traffic accidents caused by over-speeding vehicles have more causalities whereby other entities in the vicinity such as pedestrians, motorcyclists, or other vehicles might be involved in the accident. Therefore, systems for warning over-speeding vehicles would be critical to the improvement of road safety by alleviating the causalities of traffic accidents caused by over-speeding vehicles.

Currently, fixed speed detectors are found on the roads in developed countries, their main role is to capture any vehicle that exceeds the speed limit on the particular point and probably fine the over-speeding vehicle/driver. Conversely, those fixed infrastructures seem not to have any effect on the over-speeding issue since the drivers can use the navigation systems or warning signs to know where those cameras are located and reduce their speed for the sake of not being fined [7]. Nevertheless, using the vehicular communications, the entities in the vicinity of an over-speeding vehicle can be alerted or warned to avoid major causalities in case of traffic accidents.

Lately, intelligent transportation systems (ITS) has received the attention of both the industry and academia through various projects [8]. The main goal is to offer a variety of road services through the cloud based vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications. Actually, V2V is set to be more useful for localized emergency services while V2I is considered for non critical services [9]. However, the cloud based vehicular networks' solutions present numerous issues related to transmission of significant real-time traffic data from the roads infrastructures to the cloud servers which cause time delays and very costly in terms of bandwidth [10]. Additionally, the IEEE 802.11p Long-Term Evolution (LTE) standards, that were initially proposed for vehicular communications, revealed scalability and mobility support issues for vehicular communications [11]. Thus, the 5G cellular networks is predicted to empower ITS based services through its features including *massive bandwidth, massive connectivity* and *reduced latency* [12] [13].

Recently, a new computing paradigm referred as fog computing was presented. This computing architecture stretches the conventional cloud computing and respective services to the network level. This paradigm offers several features including low latency, extensive geo-distribution, position awareness, enhanced mobility coupled with real time service processes [14]. Contrary to the convectional central cloud-based systems, the fog based model allows the sensors to transmit the data to nearest fog devices. Those fog devices can perform computation on the collected data and help for decision making [15]. While the integration of fog computing and 5G cellular networks come to fruition, privacy and security issues should be carefully addressed. This appeals for an innovative design of secure and privacy preserving protocol for potential critical services in 5G fog based vehicular networks. In this paper, we present a secure and privacy preserving protocol for collision avoidance system with the feature of fog devices that will enable the data recorded by the vehicles speed sensors to be aggregated and sent to the neighboring entities in the vicinity of the violating vehicle. This would reduce the causalities of traffic accidents caused by over-seeding vehicles. To the best of our knowledge, this is the first study that address specific security and privacy preserving issues for collision avoidance through an over-speeding reporting system in 5G fog based vehicular networks. For a such application to gain people's consideration and motivate the stakeholders for implementation, security requirements should be satisfied. Beyond the routine security objectives such as confidentiality and authentication; it is crucial to protect the real identities of some entities in the system that send/receive the reporting messages including the vehicles, the pedestrians or the motorcyclists. For instance, the transmitted messages reporting the over-speed vehicle should not be accessed by unauthenticated entities on the roads. The system should satisfy mutual authentication between the speed sensors, the fog devices, the roadside clouds as well as the trusted entities. Also, the system should be feasible by demonstrating an acceptable lightweightness in terms of communication and computation overhead.

Taking into account the heterogeneous architecture of 5G cellular networks, the promising merits of fog computing, the security objectives to be achieved, we are encouraged to design a secure and privacy preserving protocol that enable collision avoidance by reporting the over-speeding vehicle to address the aforementioned challenges. The motivation behind this paper are as follows:

- Current vehicles are already equipped with several sensors but the information collected by the sensors are not fully utilized in real time. Depending on the type of the sensor, the collected information represents different levels of sensitivity. For example, over speeding and sudden braking data could be used differently. In this research, we consider the speed recording sensor that contains information which could be collected, analyzed, and transmitted to other entities (vehicles, pedestrian, motorcyclist) in the same vicinity as the speeding vehicle for further precautions.
- The privacy and security properties of the speeding vehicle, the roadside clouds, the fog devices, even other vehicles in the same range and direction should be met.

Consequently, the contribution of this paper are threefold:

- We first present an application model for secure and privacy preserving collision avoidance system in 5G fog based Internet of Vehicles which allows the vehicles' speed sensors to send the recorded traffic violation reports (TVR) to fixed fog nodes. The fog nodes aggregate the received reports and anonymously notify the entities in the vicinity. TVRs are then sent to other fog nodes and to road side clouds. We define the attack model of our application model and the requirements to be met by the proposed protocol in terms of security and performance.
- We design a secure and privacy preserving collision avoidance protocol in 5G fog based Internet of Vehicles based on the techniques of certificateless aggregate signcryption, pseudonymous and batch verification techniques.
- We provide the analysis of the proposed protocol in terms of security and performance. We further evaluate the performance of our protocol through computational delay, transmission overhead and simulation.

The remainder of the paper is organized as follows. We first present the related work, the system model and cryptographic primitives for constructing the proposed scheme in section 2, 3 and 4 respectively. We present the design of the proposed protocol in section 5. We discuss security and performance of the proposed protocol in section 6 and draw the conclusion in section 7.

2. Related Work

In this section, we first overview the conventional VANETs to the 5G enabled Internet of Vehicles. Then we outline the fog networking architecture and then provide available literature for secure collision avoidance systems in vehicular networks.

2.1. VANETs, 5G-Enabled Internet of vehicles

Vehicular ad hoc netwoks (VANETs) extends the conventional Mobile ad hoc networks (MANETs) [16]. In VANETs, the key entities represent the vehicles, the fixed infrastructures on the roads named road side units (RSU) and a third party named Trusted Authority (TA) responsible for the registration, certification and revocation of the entities participating in the VANETs architecture. Conventional VANETs offers two major communication techniques using the dedicated short range communication (DSRC) which are; vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications [17] [18]. Several applications were projected to be implemented through the VANETs framework, however the computational overhead of the applications in VANETs necessitates sufficient computation capabilities that appealed for the mixture of VANETs with cloud computing [19] [20]. The feasibility of VANETs integrated to cloud computing also called *Internet of Vehicles* was adopted by several researchers [21]. Nevertheless, some drawbacks were drawn among the available technologies for vehicular networks. For instance, the IEEE 802.11p has been proved by the researchers to suffer from mobility support [22].

Furthermore, the Long Term Evolution (LTE) in the 4G cellular networks does not provide required latency required for the vehicular networks [23] [24]

[25]. Hence, the key features of 5G cellular network in terms of latency, massive connectivity, spectral efficiency and data rate establish a promising paradigm for the (ITS) [26].

2.2. Fog Computing

Lately, several researchers have documented the state of art of fog computing and presented the IoT applications which could benefit from the fog networking including smart city, smart health care and smart grid [27] [28]. The merits of fog computing which aims at relieving the computation and communication burden on the cloud computing, providing an intermediate layer between the cloud and mobile/fix devices to offer smooth and law latency delivery services, were adopted [29] [30]. Yi et al., introduced possible latency sensitive application areas including real time video services, content delivery and caching, and big data analysis [31]. The authors pointed out two main issues related to resource management and computation offloading. Dantu et al., gave a comparison of fog computing and the conventional cloud computing based on energy consumption and latency [32].

In [33] Tao et al. presented the integration of fog networking and cloud computing to avail 5G-enabled Vehicle to- Grid (V2G) networks which would facilitate several V2G network. The authors also showed that fog networking can achieve 20% and 90% for time response reduction for users and data traffic respectively. For vehicular communications, fog computing has been adopted by several researchers as a promising technology to implement real time services [34] [35] [36]. In [37], Lingling et al. presented a secure and privacy preserving navigation scheme by using special crowd sourcing in Fog assisted VANETs. In this scheme, the fog devices use traffic information collected from the vehicles to compute optimal route. Thus the vehicles can get optimal routes continuously from the fog devices. For edge computing in internet of things including internet of vehicles, several research have been proposed recently. Min Chen and Yixue Hao examined the task offloading issue in ultra-dense network in order to minimize the delay while gaining the battery life [38]. In [39], the authors suggested a joint mobility-aware caching and Small Base Station (SBS) density placement scheme based on the user mobility. For the IoV, a new architecture named Cognitive Internet of Vehicles (CIoV) that focus on intra-vehicle, inter-vehicle and beyond-vehicle network was proposed [40]. Zhang et al., proposed software defined network (SDN) based concept that enhance traffic safety by detecting the driver's fatigue detection [41]. In [42], Chen et al., proposed an Edge-Cognitive-Computing architecture for smart-healthcare system that help to analyze and monitor the health of patients cognitive computing. Though the above articles tackle several issues related to edge computing,there is no comprehensive, secure and privacy preserving scheme in the literature that addressed the security and privacy threats for collision avoidance through over-speeding scenario in 5G fog based vehicular networks.

2.3. Collision Avoidance System

Collision avoidance systems (for pedestrian or other entities on the road) can be divided into three groups: Infrastructure based systems that focus on availing innovative transport infrastructures that allow the separation of cyclists, pedestrians or vehicles. Passive collision avoidance system aiming at reducing the damages after a collision such as road bumpers. Active collision avoidance system that use detection systems and sensors to alert drivers of potential accidents [43] [44] [45]. The active collision systems can also be divided in three groups: wireless, radar and vision based technologies. The radar and vision based systems are affected by numerous limitations such as recognition latency, weather, line of sight and so on. Thus, wireless based technologies can overcome the limitations of radar and vision based technologies. Recently, several manufacturers started to equip the vehicles with a set of sensors including the vehicle speed sensor (VSS), carbon monoxide sensor (CMS), alcohol sensor (ALS), Gas leakage sensors (GLS), vehicle noise sensors (VNS), ect,.. [46]. The data collected through the sensors are still strictly used within the vehicles and do not benefit neither the surrounding entities (vehicles, pedestrian, motorcyclist,..) nor the transportation authorities which would use it for several purposes [47].

Jang et al., presented a fixed sensor based intersection collision warning system [48]. Their protocol makes use of vehicle's location, speed and time collected from several sensors located at the intersection to warn for an eventual collision in the intersection. However, their article focused on collaborative intersection collision warning system rather than over-speed reporting. Additionally, the authors did not address the security and privacy concerns of the proposed protocol. For traffic violation monitoring, Mallissety et al. [49], proposed a traffic violation monitoring system in VANETs. However, their protocol was not built under the heterogeneous 5G fog based architecture and the security and privacy features were not deeply investigated.

Considering the above discussion, it is obvious that the proposed solutions in the literature do not address the reporting of speed violators tha can relieve the damages in case of accidents, and also the proposed solutions do not take advantage of 5G fog based framework which provide low latency services for ITS. As a result, it is arguable that there is not direct research in the literature that designed a secure and privacy preserving collision avoidance system in an heterogeneous 5G fog based Internet of Vehicles.

3. System Models and Design Goals

This section includes the system model, the communication model, the adversary model, the security requirements and finally the design goals.

3.1. System Model

This system mode is made by a master overviewer TA, the road side cloud (RSCs), aggregator fog device (AFD) and the speed sensors (SS) that are incorporated in the vehicles as shown in Fig. 1. We describe the role of each entity in the following:

- Transportation Authority (TA): TA is a fully trusted public agency that registers all entities in the system (SS, AFD and RSC) and provides cryptographic materials during the system initialization.

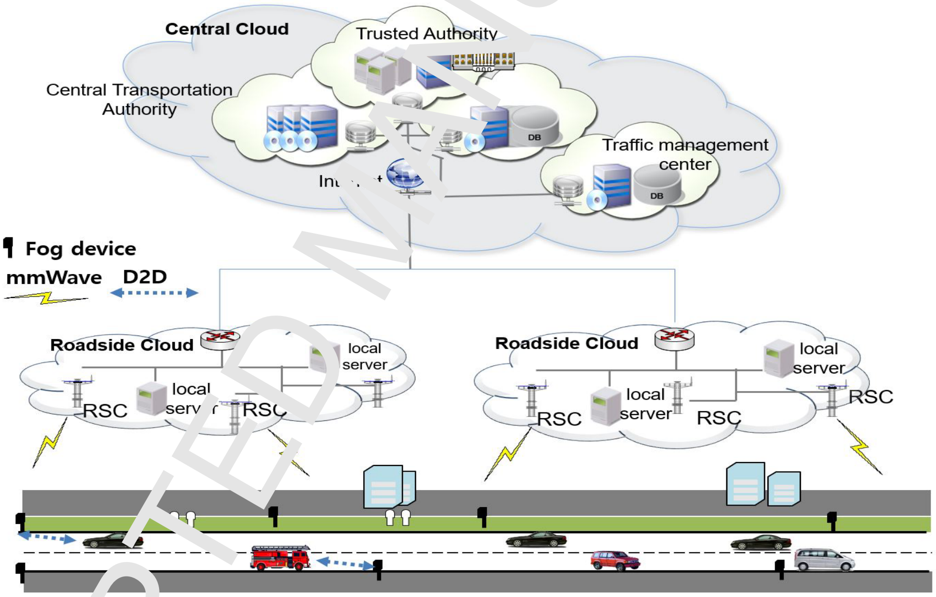

Figure 1: System Architecture

- Speed Sensing Nodes (SS): SS also denoted as $SS = \{SS_1, SS_2, ...SS_n\}$ (where n symbolize the number of sensors that send the traffic violation report on a given time) are in-built speed sensor in the vehicle. These sensors use available GPS data to know the vehicle speed limit within a location. These sensors could also be portable devices such smart phones or tablets. The sensing nodes are accountable for sending the traffic violation reports to the aggregator fog devices (AFDs).

- Aggregator Fog Devices(AFD): Like a lightweight server, AFDs are devices fixed all along the roads with computing, storage and communication capabilities. For example, they can be fixed on the road light poles. The AFDs are connected wirelessly to speed sensing nodes. The main tasks for the AFDs are; to collect the TVRs, aggregate them and perform signature verification on aggregated TVRs. The over-speed warning messages are broadcast to all authorized surrounding entities, then forwarded to other AFDs and eventually to the RSCs.

- RoadSide Cloud (RSC): RSCs are databases fixed along the roads and communicate with the AFDs. The RSCs store the traffic violation report (TVR) sent by the AFDs. Then the TVR can be sent to the TA for further legal pursuit. The RSC can also if needed broadcast the valid (aggregated and verified) TVRs. RSCs are assumed to be connected to an electricity power generator with sufficient computational capability.

- Vehicles: We assume that all the vehicles are equipped with speed sensors and connected to GPS in order to know the speed limit in a given area. The OBU collects the data through the SS and sends them to AFD using D2D or mmWave communications. All vehicles are supposed to register with the TA where periodical inspection usually takes place. Beyond the conventional identifier of the vehicle including the Electronic License Plate (ELP) or Electronic Chassis Number (ECN), each vehicle in the system is assumed to have a 5G unique identifier (5GID), similar to the mobile phone subscriber identification module (SIM) number within the conventional 3G and 4G cellular networks.

3.2. Communication Model

Motivated by the 5G cellular networks architecture, the proposed 5G fog based Internet of Vehicles is made by the following components:

- Heterogeneous Networks: This network aims at achieving high data rate and network capacity for the 5G fog based network. Therefore, two alternatives may help to get the mentioned capacities through smaller cells which increase the spectral efficiency [50]; and using the mmWave spectrum would offer high data rates since it operates within the range of 30–300 GHz and 1–10 mm for the spectrum and wavelength respectively [51].
- D2D Communications: D2D communication would enable the speed sensors to communicate with each fog device within the licensed cellular bandwidth without considering the Base stations. In the 5G fog based vehicular networks, the communication between the vehicles, speed sensors and fog devices can be done through D2D communication or mmWave technology.

In the protocol's system model, the first phase concerns the communication between the SS (speed sensor) nodes and the AFDs (aggregator fog device). The communication between those two entities is made possible through the D2D or mmWave technologies. However, we also assume that the existing and inexpensive WiFi technologies would be used in remote areas where the 5G cellular networks are not available. On the other hand, the second phase in our system model concerns the communication between the AFDs and the RSCs. Since the distance between those entities could be significant, the communication channel could be a wired or wireless link that offer low delay along with high bandwidth. In our system model, we adopt the following assumptions:

- We assume that the TA has sufficient storage capabilities, strongly protected and hard to be compromised by an adversary. TA is responsible for generating all key pairs both for the SSs, the AFDs and RSCs during the system setup phase. TA can also maintain the list of compromised entities (vehicles, fog nodes or RSCs).

- There exist one RSC in an area of 600 meters of radius which is trustworthy. RSC is responsible for keeping the TVRs for further purposes. We assume that there are at least four AFDs between two RSCs.
- Every SS sensor node communicates with exactly one or several AFD. AFD is responsible for the aggregation and verification of TVRs. AFD broacast TVRs and send them to RSCs for further purposes.
- We assume that all the entities in the system have clocks for generate time stamps and to check time validity of exchanged messages. One of the existing solution is the use of GPS satellite for time source synchronisation [52].

3.3. Adversary model

The full adoption of such application partly relies on how the security threats are handled; thus it is important to study and address all the means which the adversary can use to confuse the whole system. Within our system model, we assumed that the RCSs and AFDs are honest, but curious entities. Nevertheless, there could be an adversary near the AFDs that could eavesdrop on the TVRs. Additionally, an adversary A could also access the personal information of the vehicles through the AFDs databases. The adversary could also be able to launch different attacks such as false injection attack to threaten the integrity of the TVRs. The unauthorized access to the vehicle's personal information would lead to privacy violation. Impersonation and masquerading attacks would also lead to traffic jam since other vehicles in the same vicinity as the violating vehicle would be taking preventive actions to avoid any damages which could be caused by the violator.

3.4. Design Goals

In this section, we describe the design goals of the proposed protocol which comprise the security objectives and the performance objectives.

3.4.1. Security Objectives

- *Privacy preservation*: The SSs involved in sending the TVRs should be protected from revealing their sensitive personal data such as their respective identities. Additionally the real identities of other entities in the system that process TVRs should be preserved.

- *Mutual authentication*: The ADFs and the SSs should authenticate each other to avoid that an external and malicious user would interfere and jeopardize the system.

- *Data Confidentiality and Integrity*: All transmitted TVRs should be delivered unaltered.

- *Authorization*: The TVRs should be sent by legitimate SSs only and processed by legitimate AFDs.

- *Key Escrow Resilience:* The trusted authority and the motor department which generate the keys should not have the full private keys of all the entities in the system. Therefore, even though those key generation centers are compromised, the adversary can not get the full private keys of the entities.

- *Traceability*: The TA should be able to reveal the real identities of all the participating entities in case of dispute.

3.4.2. Performance Objectives

- Communication and verification Overhead: The secure protocol should be efficient in terms of communication overhead and offer suitable processing latency. A significant number of TVRs should be verified, aggregated in a very short interval.

- Robustness: Though some of the entities may be intruded, the TVRs sent from the SSs to the ADFs should not be accessed.

- Lightweight: Vehicle speed sensors and fog devices have limited power and storage capabilities. Thus, the proposed protocol should have low computational cost.

3.5. Overall Protocol Description

From the above described architecture, our secure and privacy preserving protocol for collision avoidance system is made by the following sub phases as shown in Fig. 2:

- Initialization: TA sets up its master secret key and its corresponding public key. Each vehicle provides its real identity and TA generates the corresponding pseudo identity for the SS from which a partial signing key is generated. AFD and RSC provide their real identities and TA assign the partial private keys. All the entities in the system including the SSs, AFDs, RSCs register with the TA.

- Traffic violation report generation and sending: When a vehicle enters a particular road, we assume that the speed sensor registers the specific accepted speed limit. Whenever a vehicle goes beyond the specified speed limit, the OBU gets the information from the speed sensor, composes message on which the OBU signcrypts. The message is sent to the closest AFD.

- TVRs aggregation and verification: Upon receiving the TVRs, the AFD performs the TVRs aggregation and verification. Since a single AFD can receive multiple TVRs simultaneously, AFD aggregate the TVRs for fast processing. Later on the AFD performs the signature verification on aggregated TVRs. This will help to discard all the bogus TVRs which might have been sent.

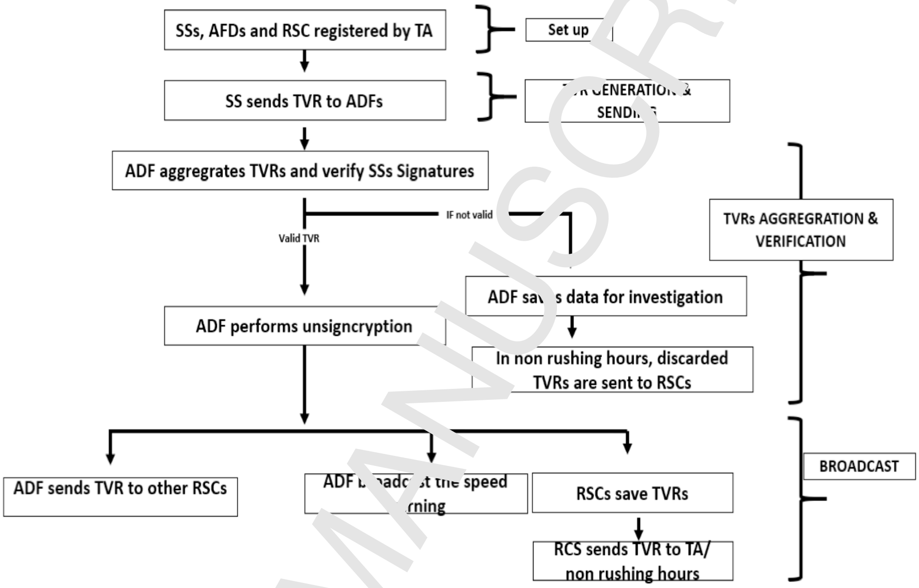
SSs, AFDs and RSC registered by TA
Set up
SS sends TVR to ADFs
TVR GENERATION & SENDING
ADF aggregrates TVRs and verify SSs Signatures
IF not valid
Valid TVR
TVRs AGGREGRATION & VERIFICATION
ADF saves data for investigation
ADF performs unsigncryption
In non rushing hours, discarded TVRs are sent to RSCs
BROADCAST
ADF sends TVR to other RSCs
ADF broadcast the speed warning
RSCs save TVRs
RCS sends TVR to TA/ non rushing hours

Figure 2: System Flowchart

- Traffic violation Report Beaconing: In case everything holds, the AFD reformulates the TVRs by removing personal information in the message that can compromise the security and identity of the sender and broadcast the speed warning. Simultaneously, the AFD forward the message to the closest AFD which will also broadcast the reformulated TVRs. In case the receiving AFD is close to an RSC, it will also forward the message to the RSC which will be later sent to the regional traffic authority (TA). Though the described protocol preserves the privacy of the road violators, the TA registers their identities for further pursuit.

4. Preliminaries

In this section, we described the certificateless scheme of signcryption (CLSC) [53] and bilinear paring [54] which are considered as our building blocks. In our construction we have used pseudonymous identity for the vehicles' speed sensors to preserve their real identities. The CLSC scheme was adopted to suit our system model for the following reasons:

1. CLSC does not use certificate for authorization. Thus, the system can avoid computational overheads caused by certificate revocation, storage and distribution.
2. In CLSC, the full private key of the users are not generated by the TA. Since the system can be deployed countrywide through regional transportation authorities, this would prevent the collapse of the whole system in case one regional transportation authority is compromised.
3. CLSC performs both signature and encryption in a single step, this helps the protocol to be lightweight which is a crucial feature for the adoption of such application.

4.1. Bilinear Maps

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of some large prime order q. The bilinear map ê: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ satisfies the following properties:

- Bilinear: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$, for all $P, Q \in \mathbb{G}_1$ and all $a, b \in \mathbb{Z}_q^*$.
- Non-degenerate: If P is a generator of $\mathbb{G}_1$ then $\hat{e}(P, P)$ is a generator of $\mathbb{G}_2$.
- Computable: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in \mathbb{G}_1$.

4.2. Certificateless Aggregate Signcryption

In the following section, we describe the main functions of the proposed protocol based on the CLSC in [53]. Those functions include the setup, partial public key generation, partial private key generation, full private key generation, signcryption, aggregation, aggregate-verification and aggregate-unsigncryption.

4.2.1. Set up [Cas.Setup()]

Let $\mathbb{G}_1$ be a cyclic additive group with a prime order q on elliptic curve, and P be an arbitrary generator of $\mathbb{G}_1$. Let $\mathbb{G}_2$ represents a cyclic multiplicative group satisfying a bilinear map where $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. $Cas.Setup()$ is executed by the TA and output the parameters as follows:

1. Randomly selects a master private key $s \in \mathbb{Z}_q^*$ and compute the master public key $P_{Key} = sP$. Note that the master private key s is kept securely by the overwiewer TA.
2. Chooses four hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*, H_2 : \{0,1\}^* \rightarrow \{0,1\}^n$ with n being the bit-length for the plaintexts to be secured. $H_3 : \{0,1\}^* \rightarrow \mathbb{G}_1$ and $H_4 : \mathbb{Z}_q^* \rightarrow \mathbb{G}_1$.
3. Set $Cas.params = (\mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, q, P_{pub}, H_1, H_2, H_3, H_4)$

4.2.2. Partial public Key Generation Algorithm [Cas.PUK()]

$Cas.PUK()$ is computed by the user VID_i to generate a partial public key as follows

1. VID_i randomly chooses $x_i \in \mathbb{Z}_q^*$ as a secret value and generates a partial public key $K_{ib} = x_i P$.
2. VID_i forwards its identity and the partial public key (VID_i, K_{ib}) to TA.

4.2.3. Partial Private Key Generation [Cas.PVR()]

$Cas.PVR()$ is run by the TA to generate a partial private key as follows:

1. TA chooses $y_i \in \mathbb{Z}_q^*$ and compute additional partial public key for VID_i as $K_{ia} = y_iP$. Then the complete public key for the vehicle becomes (K_{ib}, K_{ia}).
2. TA generates the partial private key $D_i = y_i + s * PID_i$ where $PID_i = H_1(VID_i)$. (PID_i, D_i) is sent to VID_i in a secure manner.

4.2.4. Full Key Set Algorithm [Cas.Skey()]

$Cas.Skey()$ is performed by the user VID_i after the verification of the partial private key provided by the TA:

1. VID_i checks the legitimacy of the partial private key by verifying whether $D_iP = K_{ia} + P_{key}H_1(VID_i)$ and set the full private key as (x_i, D_i).

4.2.5. SignCryption Algorithm [Cas.SignE()]

Given a message m_i, an aggregation keyword $\triangle$, *Cas.SignE()* is executed by VID_i along with the receiver ID ID_R . VID_i performs the following:

1. VID_i selects $r \in \mathbb{Z}_q^*$ and generates $T_i = rP$.
2. Compute $Z_b = rY_{rb}$.
3. Compute $Z_a = r(Y_{ra} + P_{key}PID_i)$.
4. Compute $h_a = H_2(ID_R||Y_{ra}||Y_{rb}|| \triangle ||T_i||Z_b||Z_a)$
5. Compute $F_i = h_a \bigoplus m_i$.
6. Compute $h_b = H_3(ID_R||Y_{ra}||Y_{rb}| \triangle ||T_i||F_i||PID_i||K_{ib}||K_{ia})$.
7. Compute $h_c = H_4(\triangle)$.
8. Compute $\alpha_i = D_ih_c + rh_b + x_ih_c$.
9. Return the ciphertext $C_i = (T_i, F_i, \alpha_i)$.

4.2.6. Aggregation Algorithm [Cas.Aggr()]

Taking the receiver ID ID_R, *Cas.Aggr()* is executed by the receiver through the following steps:

1. Generates $\alpha = \sum_{i=1}^{n} \alpha_i$
2. Returns $C = (T_1 ... T_n, F_1 ... F_n, \alpha)$.

4.2.7. Aggregation-Verification Algorithm [Cas.AggrV()]

The receiver ID_R runs *Cas.AggrV()* by computing the following:

1. Compute $h_b = (ID_R||Y_{ra}||Y_{rb}|| \triangle ||T_i||F_i||PID_i||K_{ib}||K_{ia})$ for $i = 1, ...n$
2. Compute $h_c = H_4(\triangle)$
3. Compute the verification by running $\hat{e}(\alpha, P) = \hat{e}(\sum_{i=1}^{n} K_{ia} + P_{key}PID_i, h_c)\hat{e}(\sum_{i=1}^{n} T_ih_b)\hat{e}(\sum_{i=1}^{n} K_{ib}, h_c)$.
   The correctness is verified as follows

$(\alpha, P) = \hat{e}\Big(\sum_{i=1}^{n} \alpha_i, P\Big)$

$= \Big(\sum_{i=1}^{n}(D_i h_c + r h_b + x_i h_c), P\Big)$

$= \Big(\sum_{i=1}^{n} D_i h_c, P\Big)\hat{e}\Big(\sum_{i=1}^{n} rP, h_b\Big)\hat{e}\Big(\sum_{i=1}^{n} x_i P, h_c\Big)$

$= \Big(\sum_{i=1}^{n} D_i P, h_c\Big)\hat{e}\Big(\sum_{i=1}^{n} T_i, h_b\Big)\hat{e}\Big(\sum_{i=1}^{n} K_i b, h_c\Big)$

$= \Big(\sum_{i=1}^{n} K_{ia} + P_{pub} PID_i, h_c\Big)\hat{e}\Big(\sum_{i=1}^{n} T_i h_b\Big)\hat{e}\Big(\sum_{i=1}^{n} K_{ib}, h_c\Big)$ If all the equations hold, it outputs true, otherwise false.

4.2.8. Aggregation-Unsigncrypt Algorithm [Cas.AggrV()]

In case *Cas.AggrV()* holds, the receiver ID_R performs the following to unsigncrypt the ciphertext:

1. Compute $Z_b^{'} = x_r T_i$
2. Compute $Z_a^{'} = D_r T_i$
3. Compute $h_a^{'} = H_2(ID_R||Y_{ra}||Y_{rb}|| \triangle ||T_i||Z_b^{'}||Z_a^{'})$
4. Compute $K_i \bigoplus h_a^{'}$
5. Finally, it outputs $\{m_i\}_{i=1}^{n}$. The correctness is verified as follows

$\mathrm{m}_i^{'} = F_i \oplus h_a^{'}$

$= \mathrm{H}_2(PID_i||K_{ia}||K_{ib}|| \triangle ||T_i||Z_b||Z_a) \oplus m_i \oplus h_a^{'}$

$= \mathrm{h}_a \oplus m_i \oplus h_a^{'}$

$= m_i$

5. Proposed Protocol

In this section we present a secure and privacy preserving collision avoidance system for 5G fog based Internet of Vehicles which is made by following main sub protocols: system initialization, traffic (speed) violation report(TVR) generation and sending, TVR aggregation and verification and TVR broadcast. The list of notations within the protocol are found in Tab. 1

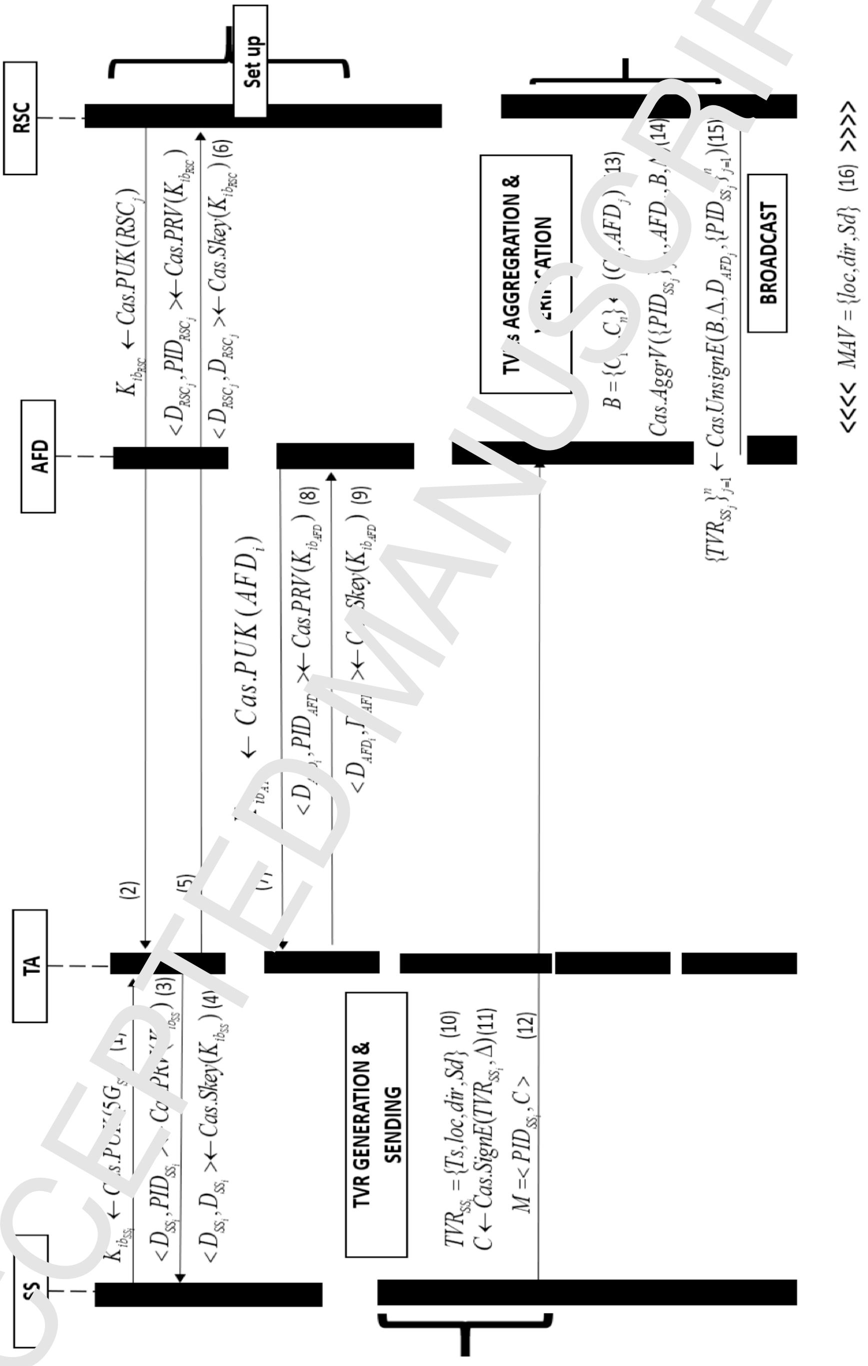
SS
TA
AFD
RSC
Set up
$K_{ib_{RSC}} \leftarrow Cas.PUK(RSC_j)$ (2)
$<D_{RSC_j}, PID_{RSC_j}> \leftarrow Cas.PRV(K_{ib_{RSC}})$ (5)
$<D_{RSC_j}, D_{RSC_j}> \leftarrow Cas.Skey(K_{ib_{RSC}})$ (6)
$\leftarrow Cas.PUK(AFD_i)$ (7)
$<D_{AFD_i}, PID_{AFD}> \leftarrow Cas.PRV(K_{ib_{AFD}})$ (8)
$<D_{AFD_i}, D_{AFD}> \leftarrow Cas.Skey(K_{ib_{AFD}})$ (9)
$K_{ib_{SS_i}} \leftarrow Cas.PUK(5G_{SS_i})$ (1)
$<D_{SS_i}, PID_{SS_i}> \leftarrow Cas.PRV(K_{ib_{SS}})$ (3)
$<D_{SS_i}, D_{SS_i}> \leftarrow Cas.Skey(K_{ib_{SS}})$ (4)
TVR GENERATION & SENDING
$TVR_{SS_i} = \{Ts, loc, dir, Sd\}$ (10)
$C \leftarrow Cas.SignE(TVR_{SS_i}, \Delta)$ (11)
$M = <PID_{SS_i}, C>$ (12)
TVRs AGGREGRATION & VERIFICATION
$B = \{C_1, ..., C_n\} \leftarrow (C, AFD_j)$ (13)
$Cas.AggrV(\{PID_{SS_j}\}, AFD, B, \Delta)$ (14)
$\{TVR_{SS_j}\}_{j=1}^{n} \leftarrow Cas.UnsignE(B, \Delta, D_{AFD_j}, \{PID_{SS_j}\}_{j=1}^{n})$ (15)
BROADCAST
<<<< $MAV = \{loc, dir, Sd\}$ (16) >>>>

Figure 3: Protocol description

Table 1: Notations and Descriptions

Notation	Description
$5G_{SS_i}$	Unique 5G identity for each sensor i
TA	Trusted Authority
s_{TA}	Trusted Authority private key
RSC_j	Roadside cloud's server
AFD_i	Identity of aggregator fog device
$\triangle$	Location based keyword
TVR	Traffic(speed) violation report
K_{ib_j}	Partial public key for an entity j
D_i	Private key of entity i
s_i	Full private key of entity i
PID_i	Pseudo identity for an entity i
Ts	time stamp
Sd	vehicle speed
dir	vehicle direction
loc	vehicle location
TVR	Traffic(speed) violation report
$\mathbb{G}_1$	Elliptic curve group with the same order q
$P \in \mathbb{G}_1$	A generator of $\mathbb{G}_1$
VAM	Violation alarm message

5.1. Initialization

Within this setup phase, TA generates the general parameters and the other entities register to TA. Note that some steps such as the generation of the TA's master secret key are not described in Fig. 3:

- *Step 0.* TA selects an elliptic curve group $\mathbb{G}_1$ of order q and a generator $P \in \mathbb{G}_1$. TA computes the master secret s_{TA} and public key P_{TA} by running $Cas.Setup()$ and set $< s_{TA}, Cas.params > \leftarrow Cas.Setup()$, then publishes the parameters $Cas.params$.

- *Step 1.* Each speed sensor SS_i runs $K_{ib_{SS_i}} \leftarrow Cas.PUK(5C_{SS_i})$ to generate its partial public key and sends it to TA.

- *Step 2.* RSC_j generates $K_{ib_{RSC_j}} \leftarrow Cas.PUK(RSC_j)$ as its partial key and sends it to TA.

- *Step 3.* TA generates $< D_{SS_i}, PID_{SS_i} > \leftarrow Cas.PVR(K_{ib_{SS_i}})$ as the partial private key of SS_i and sends it to SS_i .

- *Step 4.* SS_i set its full private key by running $< s_{SS_i}, D_{SS_i} \leftarrow Cas.Skey(D_{SS_i}) >$.

- *Step 5.* TA generates $< D_{RSC_j}, PID_{RSC_j} > \leftarrow Cas.PVR(K_{ib_{RSC_j}})$ as the partial private key of RSC_j and sends it to RSC_j.

- *Step 6.* RSC_j runs $< s_{RSC_j}, D_{RSC_j} \leftarrow Cas.Skey(D_{RSC_j}) >$ to set its full private key.

- *Step 7.* Each aggregator fog device AFD_i generates $K_{ib_{AFD_i}} \leftarrow Cas.PUK(AFD_i)$ as its partial public key and sends it to TA.

- *Step 8.* TA generates $< D_{AFD_i}, PID_{ADF_i} > \leftarrow Cas.PRV(K_{ib_{AFD_i}})$ as the partial private key of AFD_i and sends it to AFD_i.

- *Step 9.* AFD_i runs $< s_{AFD_i}, D_{AFD_i} \leftarrow Cas.Skey(D_{AFD_i}) >$ to set its final private key.

The TA determines also the formats of TVRs sent by the SSs.

5.2. Traffic violation report generation and sending

A speed sensor SS_i will use the GPS information to know the acceptable speed limit in a given area. For instance, in a school zone the speed limit is normally [illegible]0 km/h. In such environment any vehicle driving beyond that speed limit will cause SS_i to generate a TVR and forward it to AFD_i. Suppose a speed sensor SS_i of a vehicle v_i records a TVR, it performs the following:

- *Step 12.* Compose a traffic violation message $TVR_{SS_i} = \{Ts, loc, dir, Sd\}$ where Ts, loc, dir and Sd represent the time stamp, the location, the direction and the speed respectively. SS_i will also generate a zone secret value $\triangle$ corresponding to each location based to corresponding RSC_j coverage.

- *Step 13.* SS_i generates $< C \leftarrow Cas.SignE(TVR_{SS_i}) >$.

- *Step 14.* SS_i sends $M =< PID_{SS}, C >$ to AFD_j.

5.3. Traffic violation report aggregation and verification

The aggregation protocol is responsible for to aggregate multiple ciphertext Ms into a single M. This is very important because some highways can have up to 16 lanes, 8 lanes in one side and 8 lanes in the opposite side. Even in the cities, we can easily find an 8 or 12 lanes road with 4 lanes or 6 lanes each side. Thus, hundreds of vehicles can violate the speed limit in few milliseconds. The system should be able to aggregate those TVRs and report them on time. This is very useful for timely speed violation reporting. Suppose for a set of $TVR_{SS_i} = \{T, loc, dir, Sd\}$ generated by $n < SS_1......SS_n >$, we can achieve the aggregation of several M as $Aggr_M =< PID_{SS_1}, ...PID_{SS_n}, C_1, ...C_n >$. ADF_j performs the following to aggregate the $TVRs$.

- *Step 13.* AFD_j takes $C_j = \{C\}_{j=1}^{n}$ and outputs the aggregated ciphertext $B = \{C_1, ...C_n\} \leftarrow (C_j, RSC_j)$.

- *Step 14.* AFD_j runs $Cas.AggrV(\{PID_{SS_j}\}_{j=1}^{n}, RSC_j, B, \triangle)$ for signature batch verification.

If the signature verification holds,

- *Step 15.* AFD_j outputs $\{TVR_{SS_j}\}_{j=1}^{n} \leftarrow Cas.UnsignE(B, \triangle, D_{AFD_j}, \{PID_{SS_j}\}_{j=1}^{n})$ to recover the TVRs.

5.4. Traffic violation report broadcast

- *Step 16.* After the RSC_j has successfully recover the traffic violation reports $TVR_{SS_i} = \{T, loc, dir, Sd\}$, it reformulates the message and broadcast the violation alert message $VAM = \{loc, dir, Sd\}$ which only contains the location of the vehicle, the direction and speed. As we noted in the assumption, the vehicles on board units have display facilities and able to approximately show the position of the violating vehicle on the screen. Note that the $VAMs$ can be forwarded to RSC_j for faster broadcast, also the RSC_j can play the role of AFD_j if the violating vehicle is closer to RSC_j than AFD_j.

6. Security and Performance Analysis

In this section, we evaluate the proposed protocol in terms of security goals, computational cost and communication cost.

6.1. Security Analysis

We discuss in this section the security goals for overspeed reporting in 5G fog based vehicular networks as set in section 3.4.1

1. *Privacy preservation:* The proposed protocol guaranties the identity protection of the entities participating in the system. First, an adversary can not retrieve the identity of the SS_i or the AFD_j through eavesdropping because there is no plain text within the transmitted TVR from SS_i to AFD_j since SS_i sends $M =< PID_{SS}, C >$ with $< C \leftarrow Gen.SignE(TVR_{SS_i}) >$. Also, during the registration phase, the SS_i or AFD_j is provided a partial private key with a pseudo identity $PID_i = H_1(VS_i)$. Given that the partial private key $D_i = y_i + s * PID_i$ with $PID_i = H_1(VID_i)$, which contains the pseudo identity is sent securely to the requesting entity, the adversary cannot reveal the real identity of the SS_i by eavesdropping. Additionally, assume the fog devices are compromised by the adversary, the adversary would only get the SS_i pseudo

identity which can not reveal it real identity. Therefore, we confirm that the proposed protocol achieves identity preservation.

2. *Authentication*: The authentication between SS_i and AFD_j upon sending a TVR is guaranteed by the signcryption on the TVR. After generating a speed violation message $TVR_{SS_i} = \{Ts, loc, dir, Sd\}$, SS_i performs signcryption on the message as $< C \leftarrow Cas.SignE(TVR_{SS_i}) >$. Only the entity with valid full private key can unsigncrypt the TVRs. Note that the adversary can not have the full private key of a speed sensor SS_i because even the TA does not have the full private key of the SS_i. TA only generates the partial private key of the entities by running $Cas.PVR()$. Thus, entity authentication is provided by the certificateless aggregate signcryption technique. The security of the signature depends on the *unforgeability* of CLCS scheme under adaptively chosen message attacks [53]. Consequently, we endorse that the designed protocol guaranties entity authentication.

3. *Authorization*: In the proposed protocol, an unauthorized SS_i can not send any TVRs. First the protocol prevents the malicious users outside the RSC zone to generate a TVR. As described in section 5.2, SS_i composes a traffic violation message $TVR_{SS_i} = \{Ts, loc, dir, Sd\}$ where Ts, loc, dir and Sd represent the time stamp, the location, the direction and the speed respectively. SS_i will then generate a zone secret value $\triangle$ corresponding to each location based on the RSC sites. Thus, this will prevent an adversary outside the RSC zone to generate TVRs. Additionally, even though an adversary in the zone generates a TVR, the TVR signature verification function $Cas.AggrV()$ will reject any TVR generated by an SS_i which is not registered by the TA. Therefore, the proposed protocol achieve entity authorization.

4. *Confidentiality and Integrity*: The speed sensor SS_i generates a TVR and signcrypts it as $< C \leftarrow Cas.SignE(TVR_{SS_i}) >$. Note that within the signcrypt function $Cas.SignE()$, the ciphertext contains $C_i = (T_i, F_i, \alpha_i)$ where T_i and F_i accomplishes the functionalities of message encryption

and α_i the duties of digital signature. In the proposed protocol, only the legitimates $AFDs$ can perform the unsigncryption of C_i through the computation of T_i, F_i and α_i. Therefore, since the certificateless signature is proven to be secure under adaptively chosen ciphertext (IND-CC2) [55], we confirm that the proposed protocol achieves message confidentiality and integrity.

5. *Key Escrow Resilience*: The massive connectivity of the 5G cellular networks required distributed systems to avoid key management burdens. Thus, the applications under the 5G fog based architecture ought to satisfy the *Key Escrow resiliency.* In the proposed protocol, the speed sensors generate their partial public key by computing $Cas.PUK()$. The SSs sends the partial public key to TA which will only compute the partial private key by running $Cas.PVK()$. The full private key of SS is computed by SS_i after the verification of the partial private key generated by the TA. Therefore, we confirm that the proposed protocol achieves *key escrow resilience* property.
6. *Traceability*: In the proposed protocol, the TA generates the entity pseudo identities $PID_i = H_1(SS_i)$ and saves the hash values in a table. Therefore, in case of dispute, the TA is able to reveal the real identities of the entities in the dispute by checking the corresponding hash value of the pseudo identity which was reported. Thus, we argue that the proposed protocol guaranties the traceability of the participating entities.

6.2. Performance Analysis

In this section, we provide the performance analysis of the proposed protocol based on the computational and communication cost.

6.2.1. Computational Cost

In CLSC [53], three main operations are executed; the scalar multiplication executed in group $\mathbb{G}_1$, the exponentiation operation that is calculated in the group $\mathbb{G}_2$, and lastly the pairing operation. Those three operations are respectively denoted as T_{mul}, T_{exp} and T_{pair}. However, the proposed construction only performs T_{mul} and T_{pair}. To measure the computation cost of the proposed protocol, we made use of an MNT curve along with the Tate pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2$ on the curve, the embedding degree is 6 and the q is represented by 160 bit [56]. The implementation was done on a desktop computer with 3.5GHz, core $i-5$, 16GB RAM using the pairing based library in and the Miracl library. The execution time are depicted in Tab. 2.

Table 2: Measurement of cryptographic operations

$Notation$	Operations	time (ms)
T_{pair}	Bilinear pairing	4.5
T_{mul}	Point scalar multiplication	0.6
T_{exp}	Modular exponentiation	1.4

In the proposed secure and privacy preserving collision avoidance protocol, whenever a SS_i senses a speed violation, it executes 6 T_{mul} to sign a TVR as described in section 4.2.5. On the other hand, the receiver AFD_j performs 4 T_{pair} to aggregate, verify and unsigncrypt the TVRs as shown in section 4.2.7. Fig. 4 shows the total cost of signing one or multiple TVRs. As shown in the figure, the time for verifying multiple TVRs is stable due to *batch verification technique* which is used for TVR signature verification. Thus, the proposed protocol would for instance require 18 ms to verify 1000 TVRs. For the signing process, we assume that a SS_i signs one TVRs at a go which cost 3.6 ms.

Table 3: Computational cost of proposed protocol

Scheme Phase	Operation	Cost/ms
Signcrypt TVR	$6T_{mul}$	$3.6ms$
Aggr/verify/Unsigncrypt TVR	$4T_{pair}$	$18ms$
Total		21.6

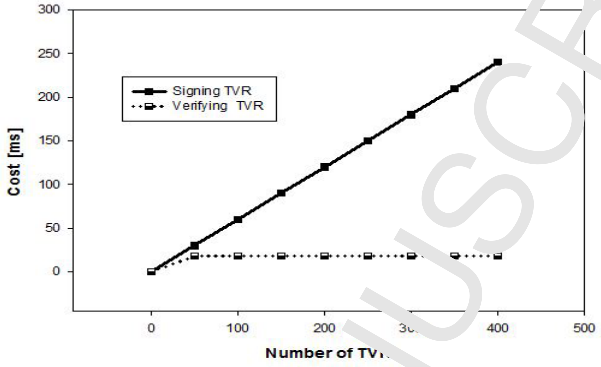

Figure 4: Overall Sign/Verification Cost of TVR

6.2.2. Communication Cost

In this section, we provide the analysis of communication cost for the secure and privacy preserving collision avoidance system. The communication cost includes the cost of transmitting the TVRs from the SS_i to the AFD_j. We first emphasize on the transmission overhead caused by the signcryption which was performed on the TVR. In $\mathbb{G}_1$, the sizes of the elements are $64 \times 2 = 128$ bytes and $20 \times 2 = 40$ bytes for $\mathbb{G}_1$. The sizes for the hash fuctions is 20 bytes and the other elements such as the time stamps have a 4 bytes size [57]. In the proposed protocol, the signcrypt function $Cas.SignE()$ contains the ciphertext $C_i = (T_i, F_i, \alpha_i)$ where $T_i = 20$ bytes, $F_i = 60$ bytes and the signature $\alpha_i = 56$ bytes. The size of the a raw warning message is 40 bytes according to the society of automotive engineers. Therefore the size of raw TVR is 40 bytes where as a secure TVR size is 136 bytes [58].

6.2.3. Simulation

In this subsection, simulation experiments are provided in two folds. First we investigate the impact of the TVR size on the computation offloading. Secondly, we investigate the impact of vehicle's speed, vehicle's density and fog device's density on the loss ratio.

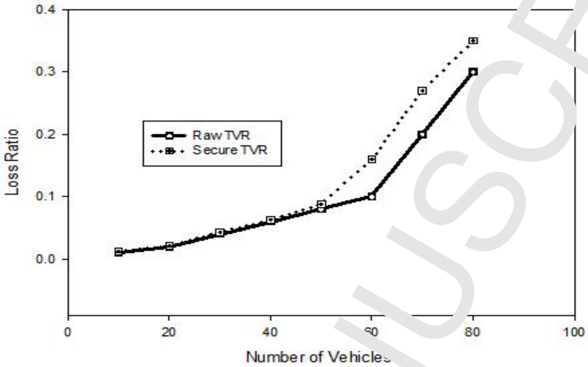

Figure 5: Impact of Number of vehicles on the average loss ratio

6.2.3.1 *Impact of TVR Size on Computational Offloading*

Assume that each AFD needs a computation amount M_i to execute a task T_{task} of a TVR of size TVR_{size}. The computing resource within edge/fog computing is set to 25 GHz and the computing resource for vehicles OBU is set to 10 GHz.As described in subsection 3.1, the vehicle's OBU could also be assumed as a mobilephone fixed in the vehicles. The distance between one RSC to another is 600 m in which we set 3 base stations (BS). We adopt *Energy Optimal (GSI)* as a benchmark algorithm because it helps the user (OBU) to connect with the best channel regardless of the delay performance. Energy Optimal (GSI) is the standard 3GPP LTE protocol for handover [59]. The size of the secure and non secure TVRs are described in Tab. 4 as calculated in subsection 6.2.2. The details of the simulation setting are set as described and suggested in [60].

We evaluate the size of the TVR with and without security features on computational offloading. As shown in Fig. 6, the larger the TVR size, the longer the task would take. However the difference is not considerable looking at the side effects which could be obtained for non secure TVR. For instance, for a 60 bytes TVR message, the task execution is is 0.5 milliseconds for unsecured message and 0.59 milliseconds for secured VTR. The overall increase is of 9 % which is not considerable. In this subsection , we neglected the investigation that output the impact of TVR size on energy cost. This is because we consider that a vehicle's OBU is not subject to energy issues since it keeps on recharging whenever the vehicle's engine is on. Additionally we also assume that the fix fog devices can also be connected to an electricity generation resource.

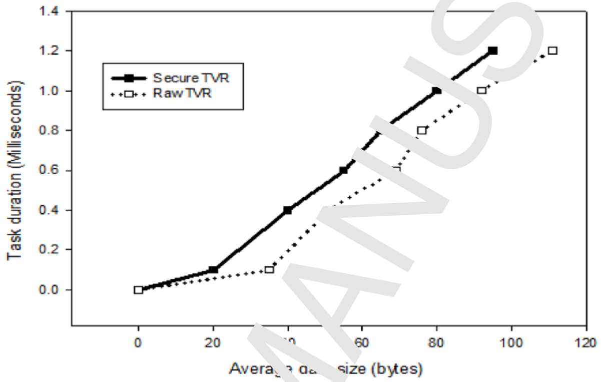

Figure 6: Impact of TVR size on the task duration

6.2.3.2 *Impact of vehicle's density and speed on loss ratio*

In addition, we make use of VANET-SIM simulator to enable vehicle mobility; then for network simulation we used ns-3 simulator [61]. We later set our system scenario using the IEEE 802.11p platforms for the 5G cellular network which is predicted to range from 1 Gbps for highly populated roads to a maximal transmission range of 9-10 Gbps [62] .

The ns-3 is set using the Friis equation that describes the propagation of signal as $P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi l)^2}$ with P_t being the transmission power, then G_t and G_r represent the antenna gains, λ represents length of the wave and l represents the distance from the receiver to the transmitter [63].

Furthermore, we downloaded a map from OpenStreepMap website [64]. In our simulation, each vehicles is randomly released and can move randomly within the map. The speed of the vehicles is set from 10 to 40 m/s that is 36 to 144 km/hr. . Tab. 4 describes more details concerning the settings for

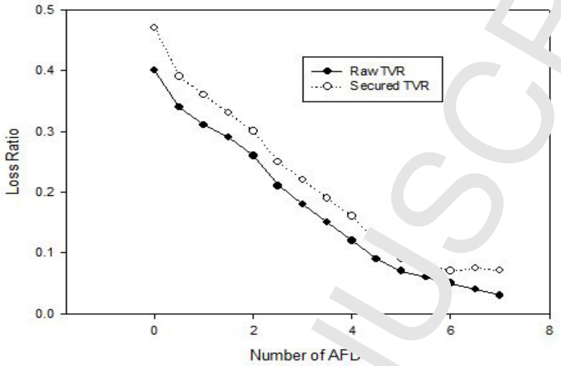

Figure 7: Impact of ADF on the average loss ratio

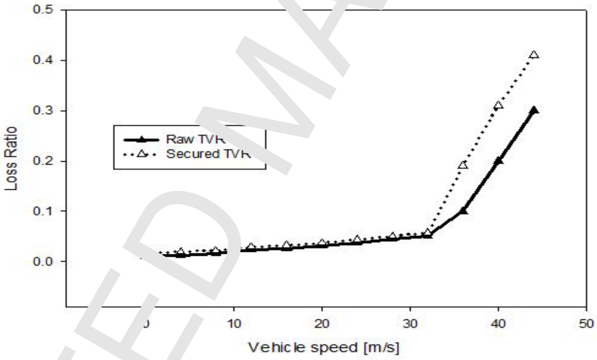

Figure 8: Impact of vehicle speed on the average loss ratio

the simulation.

We later calculated the message loss ratio (AV_R) as follows [65]:

$$AV_R = \frac{\sum_{i=1}^{DE}\sum_{j=1}^{TVR}\sum_{k=1}^{FD}(T_F - T_C)}{\sum_{i=1}^{DE} TVR} + Aver$$

where DE, TVR, FD, T_F, T_R and $Aver$ represent the density of the vehicles, the number of TVR sent by v_i, the number of AFD_j within the simulation area, the time when v_i forwards a TVR message to AFD_j, the time AFD_j receives a TVR message from v_i and the average aggregation verification time that AFD_j authenticates/aggregates and verify the TVRs respectively.

Table 4: Simulation settings

Tools/Parameter	Value/Specification
Mobility generation tool	VANETSIM 2.02
Network Simulation tool	ns-3
$Trans\ range$	$1GBps$
$Number-of-vehicle$	15
Simulation time	200 min
Wireless protocol	802.11p
TVR propagation interval	6 sec
Departure interval	20 sec
$RSC\ radius$	600 m
Number of AFD within 2 RSC	3
$mobility\ model$	$shortest\ path$
Message size for raw TVR	40 bytes
Message size for secured TVR	136 bytes

Fig. 7 shows the average loss ratio according to the number of available AFD. We can see that as the number of fog devices increases, the average loss ratio decreases. Therefore, the fog based computing within the cellular networks overcome the communication overheads of convectional vehicular networks. In Fig. 5 and 8, we show the average loss ratio based on the number of vehicles and the vehicles speed. As we can see, the raw TVR which has a smaller size performs better than a secured TVR. For instance, in Fig. 8, the loss ratio starts increasing significantly when the violating vehicles go beyond a speed of 34 m/s which is 122 km/h. In Fig. 5, the performance of the proposed protocol for secured TVR is close to raw TVR when the number of vehicles is less than 70. Thus, in urban areas where the speed limit range from 60 to 80 km/h, the computational and communication overhead caused by the security features do not affect significantly the performance of the overall system.

7. Conclusion

While we wait the fulfillment of 5G fog based internet of vehicles, security and privacy should be carefully addressed for ITS applications. Therefore, we proposed in this paper a secure and privacy preserving collision avoidance system in 5G fog based internet of vehicles. The fog devices are used to collect speed violation report (TVR) sent by the vehicles speed sensor. The batch verification techniques allow the fog devices to verify multiple TVRs simultaneously. The features of certificateless aggregate signcryption scheme that offer both the encryption and digital signature in a single step were adopted to securely transmit the speed violation reports. The proposed protocol is suitable for distributed systems since it meets not only the routine security goals as such authentication, confidentiality and integrity but also the key escrow resilience . The performance analysis in terms of computation and communication overhead confirms its efficiency.

Acknowledgment

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B03036285)

References

[1] E. Kopits, M. Cropper, Traffic fatalities and economic growth, Accident Analysis & Prevention 37 (1) (2005) 169–178.

[2] N. H. T. S. Administration, et al., Traffic safety facts: 2007 data: pedestrians, Annals of Emergency Medicine 53 (6) (2009) 824.

[3] G. Zhang, K. K. Yau, X. Gong, Traffic violations in guangdong province of china: Speeding and drunk driving, Accident Analysis & Prevention 64 (2014) 30–40.

[4] W. H. Organization, Global status report on road safety: time for action, World Health Organization, 2009.

[5] W. Barfield, T. A. Dingus, Human factors in intelligent transportation systems, Psychology Press, 2014.

[6] J. K. Lee, Y. S. Jeong, J. H. Park, s-itsf: a service based intelligent transportation system framework for smart accident management, Human-centric Computing and Information Sciences 5 (1) (2015) 34.

[7] Y. Jiang, J. Zhang, M. Chikaraishi, H. Seya, A. Fujiwara, Effects of a gps-enabled smart phone app with functions of driving safety diagnosis and warning information provision on over-speeding violation behavior on expressways, Transportation Research Procedia 25 (2017) 1820–1828.

[8] C. Wang, X. Li, X. Zhou, A. Wang, N. Nedjah, Soft computing in big data intelligent transportation systems, Applied Soft Computing 38 (2016) 1099–1108.

[9] C.-Y. Chang, H.-C. Yen, D.-J. Deng, V2v qos guaranteed channel access in ieee 802.11 p vanets, IEEE Transactions on Dependable and Secure Computing 13 (1) (2016) 5–17.

[10] X. Cao, L. Liu, Y. Cheng, L. X. Cai, C. Sun, On optimal device-to-device resource allocation for minimizing end-to-end delay in vanets, IEEE Transactions on Vehicular Technology 65 (10) (2016) 7905–7916.

[11] Z. H. Mir, F. Filali, Lte and ieee 802.11 p for vehicular networking: a performance evaluation, EURASIP Journal on Wireless Communications and Networking 2014 (1) (2014) 89.

[12] N. Zhang, N. Cheng, A. T. Gamage, K. Zhang, J. W. Mark, X. Shen, Cloud assisted hetnets toward 5g wireless networks, IEEE communications magazine 53 (6) (2015) 59–65.

[13] C.-F. Lai, Y.-C. Chang, H.-C. Chao, M. S. Hossain, A. Ghoneim, A buffer-aware qos streaming approach for sdn-enabled 5g vehicular networks, IEEE Communications Magazine 55 (8) (2017) 68–73.

[14] F. Bonomi, R. Milito, J. Zhu, S. Addepalli, Fog computing and its role in the internet of things, in: Proceedings of the first edition of the MCC workshop on Mobile cloud computing, ACM, 2012, pp. 13–16.

[15] I. Stojmenovic, S. Wen, X. Huang, H. Luan, An overview of fog computing and its security issues, Concurrency and Computation: Practice and Experience 28 (10) (2016) 2991–3005.

[16] M. Altayeb, I. Mahgoub, A survey of vehicular ad hoc networks routing protocols, International Journal of Innovation and Applied Studies 3 (3) (2013) 829–846.

[17] J. Yin, T. ElBatt, G. Yeung, B. Ryu, S. Habermas, H. Krishnan, T. Talty, Performance evaluation of safety applications over dsrc vehicular ad hoc networks, in: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, ACM, 2004, pp. 1–9.

[18] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, M. K. C. Reddy, A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for vanets, Future Generation Computer Systems 84 (2018) 216–227.

[19] R. Hussain, J. Son, H. Eun, S. Kim, H. Oh, Rethinking vehicular communications: merging vanet with cloud computing, in: 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom), IEEE, 2012, pp. 606–609.

[20] T. Kim, H. Min, J. Jung, Vehicular datacenter modeling for cloud computing: Considering capacity and leave rate of vehicles, Future Generation Computer Systems 88 (2018) 363–372.

[21] W. He, G. Yan, L. Da Xu, Developing vehicular data cloud services in the iot environment, IEEE Transactions on Industrial Informatics 10 (2) (2014) 1587–1595.

[22] B. Bellalta, E. Belyaev, M. Jonsson, A. Vinel, Performance evaluation of ieee 802.11 p-enabled vehicular video surveillance system, IEEE Communications Letters 18 (4) (2014) 708–711.

[23] E. Belyaev, A. Vinel, A. Surak, M. Gabbouj, M. Jonsson, K. Egiazarian, Robust vehicle-to-infrastructure video transmission for road surveillance applications, IEEE Transactions on Vehicular Technology 64 (7) (2015) 2991–3003.

[24] M. H. Eiza, Q. Ni, T. Owens, G. Min, Investigation of routing reliability of vehicular ad hoc networks, EURASIP journal on wireless communications and networking 2013 (1) (2013) 179.

[25] M. H. Eiza, T. Owens, Q. Ni, Q. Shi, Situation-aware qos routing algorithm for vehicular ad hoc networks, IEEE Transactions on Vehicular Technology 64 (12) (2015) 5520–5535.

[26] A. A. Mutlag, M. K. A. Ghani, N. Arunkumar, M. A. Mohamed, O. Mohd, Enabling technologies for fog computing in healthcare iot systems, Future Generation Computer Systems 90 (2019) 62–78.

[27] S. Sarkar, S. Misra, Theoretical modelling of fog computing: a green computing paradigm to support iot applications, IET Networks 5 (2) (2016) 23–29.

[28] P. Zhang, M. Zhou, G. Fortino, Security and trust issues in fog computing: A survey, Future Generation Computer Systems 88 (2018) 16–27.

[29] E. K. Markakis, K. Karras, N. Zotos, A. Sideris, T. Moysiadis, A. Corsaro, G. Alexiou, C. Skianis, G. Mastorakis, C. X. Mavromoustakis, et al., Exegesis: Extreme edge resource harvesting for a virtualized fog environment, IEEE Communications Magazine 55 (7) (2017) 173–179.

[30] Y. Zhang, H. Cai, B. Xu, A. T. Vasilakos, C. Huang, Data driven business rule generation based on fog computing, Future Generation Computer Systems 89 (2018) 494–505.

[31] S. Yi, C. Li, Q. Li, A survey of fog computing: concepts, applications and issues, in: Proceedings of the 2015 Workshop on Mobile Big Data, ACM, 2015, pp. 37–42.

[32] K. Dantu, S. Y. Ko, L. Ziarek, Raina: Reliability and adaptability in android for fog computing, IEEE Communications Magazine 55 (4) (2017) 41–45.

[33] M. Tao, K. Ota, M. Dong, Foud: Integrating fog and cloud for 5g-enabled v2g networks, IEEE Network 31 (2) (2017) 8–13.

[34] J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng, J. Shen, Secure intelligent traffic light control using fog computing, Future Generation Computer Systems 78 (2018) 817–824.

[35] C. Zhang, L. Zhu, C. Xu, K. Sharif, X. Du, M. Guizani, Lptd: Achieving lightweight and privacy-preserving truth discovery in ciot, Future Generation Computer Systems 90 (2019) 175–184.

[36] N. Verba, K.-M. Chao, J. Lewandowski, N. Shah, A. James, F. Tian, Modeling industry 4.0 based fog computing environments for application analysis and deployment, Future Generation Computer Systems 91 (2019) 48–60.

[37] X. Yang, F. Yin, X. Tang, A fine-grained and privacy-preserving query scheme for fog computing-enhanced location-based service, Sensors 17 (7) (2017) 1611.

[38] M. Chen, Y. Hao, Task offloading for mobile edge computing in software defined ultra-dense network, IEEE Journal on Selected Areas in Communications 36 (3) (2018) 587–597.

[39] M. Chen, Y. Hao, M. Qiu, J. Song, D. Wu, I. Humar, Mobility-aware caching and computation offloading in 5g ultra-dense cellular networks, Sensors 16 (7) (2016) 974.

[40] M. Chen, Y. Tian, G. Fortino, J. Zhang, I. Humar, Cognitive internet of vehicles, Computer Communications 120 (2018) 58–70.

[41] Y. Zhang, M. Chen, N. Guizani, D. Wu, V. C. Leung, Sovcan: Safety-oriented vehicular controller area network, IEEE Communications Magazine 55 (8) (2017) 94–99.

[42] M. Chen, W. Li, Y. Hao, Y. Qian, I. Humar, Edge cognitive computing based smart healthcare system, Future Generation Computer Systems 86 (2018) 403–411.

[43] A. Fernández-Ares, A. Mora, M. G. Arenas, P. García-Sánchez, G. Romero, V. Rivas, P. A. Castillo, J. Merelo, Studying real traffic and mobility scenarios for a smart city using a new monitoring and tracking system, Future Generation Computer Systems 76 (2017) 163–179.

[44] W. Turek, Erlang-based desynchronized urban traffic simulation for high-performance computing systems, Future Generation Computer Systems 79 (2018) 645–652.

[45] K. M. A. Yousef, A. Shatnawi, M. Latayfeh, Intelligent traffic light scheduling technique using calendar-based history information, Future Generation Computer Systems 91 (2019) 124–135.

[46] A. Broggi, A. Zelinsky, Ü. Özgüner, C. Laugier, Intelligent vehicles, in: Springer Handbook of Robotics, Springer, 2016, pp. 1627–1656.

[47] C. Mi, M. A. Masrur, Hybrid electric vehicles: principles and applications with practical perspectives, John Wiley & Sons, 2017.

[48] J.-A. Jang, K. Choi, H. Cho, A fixed sensor-based intersection collision warning system in vulnerable line-of-sight and/or traffic-violation-prone en-

vironment, IEEE Transactions on Intelligent Transportation Systems 13 (4) (2012) 1880–1890.

[49] S. Mallissery, M. M. Pai, N. Ajam, R. M. Pai, J. Mouzna, Transport and traffic rule violation monitoring service in its: a secured vanet cloud application, in: Consumer Communications and Networking Conference (CCNC), 2015 12th Annual IEEE, IEEE, 2015, pp. 213–218.

[50] W. H. Chin, Z. Fan, R. Haines, Emerging technologies and research challenges for 5g wireless networks, IEEE Wireless Communications 21 (2) (2014) 106–112.

[51] X. Shen, Device-to-device communication in 5g cellular networks, IEEE Network 29 (2) (2015) 2–3.

[52] K. Behrendt, K. Fodero, et al., The perfect time: An examination of time-synchronization techniques, in: Proc. 33rd Ann. West. Prot. Rel. Conf., Spokane, WA, USA, 2006, pp. 17–19.

[53] Z. Eslami, N. Pakniat, Certificateless aggregate signcryption: Security model and a concrete construction secure in the random oracle model, Journal of King Saud University-Computer and Information Sciences 26 (3) (2014) 276–286.

[54] F. Zhang, R. Safavi-Naini, W. Susilo, An efficient signature scheme from bilinear pairings and its applications, Public Key Cryptography–PKC 2004 (2004) 277–290.

[55] H. Lu, Q. Xie, An efficient certificateless aggregate signcryption scheme from pairings, in: Electronics, Communications and Control (ICECC), 2011 International Conference on, IEEE, 2011, pp. 132–135.

[56] M. Scott, Efficient implementation of cryptographic pairings, in: Online]. http://www. pairing-conference. org/2007/invited/Scott slide. pdf, 2007.

[57] D. He, S. Zeadally, B. Xu, X. Huang, An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks, IEEE Transactions on Information Forensics and Security 10 (12) (2015) 2681–2691.

[58] J. B. Kenney, Dedicated short-range communications (dsrc) standards in the united states, Proceedings of the IEEE 99 (7) (2011) 1162–1182.

[59] W. Hwang, A. Bufe, Radio resource control connection release message wait timer, uS Patent 9,794,980 (Oct. 17 2017).

[60] C. Niu, Y. Li, R. Q. Hu, F. Ye, Fast and efficient radio resource allocation in dynamic ultra-dense heterogeneous networks, IEEE Access 5 (2017) 1911–1924.

[61] A. Festag, P. Papadimitratos, T. Tielert, Design and performance of secure geocast for vehicular communication, IEEE Transactions on Vehicular Technology 59 (5) (2010) 2456–2471.

[62] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, M. Di Renzo, Safeguarding 5g wireless communication networks using physical layer security, IEEE Communications Magazine 53 (4) (2015) 20–27.

[63] M. Torrent-Moreno, P. Santi, H. Hartenstein, Fair sharing of bandwidth in vanets, in: Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks, ACM, 2005, pp. 49–58.

[64] M. Haklay, P. Weber, Openstreetmap: User-generated street maps, IEEE Pervasive Computing 7 (4) (2008) 12–18.

[65] L.-Y. Yeh, J.-L. Huang, Pbs: A portable billing scheme with fine-grained access control for service-oriented vehicular networks, IEEE Transactions on Mobile Computing 13 (11) (2014) 2606–2619.

SI on Future Generation Computer Systems

Title: Towards Secure and Privacy Preserving Collision Avoidance System in 5G Fog based Internet of Vehicles

Biographies

Lewis Nkenyereye is an Assistant Professor in the Department of Computer and Information Security, Sejong University, Seoul, South Korea. Before joining Sejong University, he was a Research Fellow at Creative Human Resource Development Program for IT Convergence, Pusan National University, Busan, South Korea. He also holds a PhD in Information Security from Pukyong National University, Busan, South Korea. He received his bachelor degree in Computer Science from Light University of Burundi, master degree in Information Technology from Uganda Christian University of Uganda in 2009 and 2012, respectively. His research spans across the wide range of security and privacy related techniques with a particular interest in the Internet of Vehicles. He is a member of IEEE.

Chi Harold Liu receives a Ph.D. degree in Electronic Engineering from Imperial College, UK in 2010, and a B.Eng. degree in Electronic and Information Engineering from Tsinghua University, China in 2006. He is currently a Full Professor and Vice Dean at the School of Computer Science and Technology, Beijing Institute of Technology, China. He also serves as the Director of IBM Mainframe Excellence Center (Beijing), Director of IBM Big Data and Analysis Technology Center, and Director of National Laboratory of Data Intelligence for China Light Industry. Before moving to academia, he worked for IBM Research - China as a staff researcher and project manager from 2010 to 2013, worked as a postdoctoral researcher at Deutsche Telekom Laboratories, Germany in 2010, and as a visiting scholar at IBM T. J. Watson Research Center, USA in 2009. His current research interests include the Internet-of-Things (IoT), big data analytics, mobile computing, and wireless ad hoc, sensor, and mesh networks. He received the Distinguished Young Scholar Award in 2013, IBM First Plateau Invention Achievement Award in 2012, and IBM First Patent Application Award in 2011 and was interviewed by EEWeb.com as the Featured Engineer in 2011. He has published more than 90 prestigious conference and journal papers and owned more than 10 EU/U.S./China patents. He serves as the Area Editor for KSII Trans. on Internet and Information Systems and the book editor for four books published by Taylor \& Francis Group, USA. He also has served as the general chair of IEEE SECON'13 workshop on IoT Networking and Control, IEEE WCNC'12 workshop on IoT Enabling Technologies, and ACM UbiComp'11 Workshop on Networking and Object Memories for IoT. He served as the consultant to Asian Development Bank, Bain \& Company, and KPMG, USA, and the peer reviewer for Qatar National Research Foundation, and National Science Foundation, China. He is a Senior member of IEEE.

JaeSeung Song is an associate professor in the Computer and Information Security Department at Sejong University. He holds the position of oneM2M Test Working Group Chair. Prior to his current position, he worked for NEC Europe Ltd. and LG Electronics in various positions. He received a Ph.D. at Imperial College London in the Department of Computing, United Kingdom. He holds B.S. and M.S. degrees in computer science from Sogang University.

SI on Future Generation Computer Systems

Title: Towards Secure and Privacy Preserving Collision Avoidance System in 5G Fog based Internet of Vehicles

Highlights

- Proposed a secure and privacy-preserving model for collision avoidance system in 5G fog based Internet-of-Vehicles (IoV)
- Constructed a secure protocol using signcryption, pseudonymous and batch verification techniques
- Security and performance analysis with respect to various metrics