sensors

MDPI

Article

Secure and Blockchain-Based Emergency Driven Message Protocol for 5G Enabled Vehicular Edge Computing

Lewis Nkenyereye [1], Bayu Adhi Tama [2], Muhammad K. Shahzad [3] and Yoon-Ho Choi [4,*]

1 Department of Computer and Information Security, Sejong University, Seoul 05006, Korea; nkenyele@sejong.ac.kr
2 Department of Mechanical Engineering, Pohang University of Science and Technology, Pohang 37673, Korea; btama@acm.org
3 Department of Computing, National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan; mkhuram.shahzad@seecs.edu.pk
4 School of Computer Science and Engineering, Pusan National University, Busan 46241, Korea
* Correspondence: yhchoi@pusan.ac.kr

Received: 5 November 2019; Accepted: 23 December 2019; Published: 25 December 2019

Abstract: Basic safety message (BSM) are messages that contain core elements of a vehicle such as vehicle's size, position, speed, acceleration and others. BSM are lightweight messages that can be regularly broadcast by the vehicles to enable a variety of applications. On the other hand, event-driven message (EDM) are messages generated at the time of occurrence such as accidents or roads sliding and can contain much more heavy elements including pictures, audio or videos. Security, architecture and communication solutions for BSM use cases have been largely documented on in the literature contrary to EDM due to several concerns such as the variant size of EDM, the appropriate architecture along with latency, privacy and security. In this paper, we propose a secure and blockchain based EDM protocol for 5G enabled vehicular edge computing. To offer scalability and latency for the proposed scenario, we adopt a 5G cellular architecture due to its projected features compared to 4G tong-term evaluation (LTE) for vehicular communications. We consider edge computing to provide local processing of EDM that can improve the response time of public agencies (ambulances or rescue teams) that may intervene to the scene. We make use of lightweight multi-receiver signcryption scheme without pairing that offers low time consuming operations, security, privacy and access control. EDM records need to be kept into a distributed system which can guarantee reliability and auditability of EDM. To achieve this, we construct a private blockchain based on the edge nodes to store EDM records. The performance analysis of the proposed protocol confirms its efficiency.

Keywords: vehicle edge computing; 5G cellular networks; blockchain; multi-receiver signcryption; security; privacy

1. Introduction

Abrupt situations on roads, such as car accidents, slippery roads, or land sliding can be reported by the vehicles using the inbuilt sensors and devices. Reporting emergency situations can be an effective approach in situations where the evident proofs are required such as car accidents or reckless driving. Those reports can also provide additional materials like pictures, videos, audios to the rescue departments for an efficient and timely intervention [1]. Emergency warning can be divided in three categories; (1) a vehicle-to-vehicle (V2V) warning dissemination such as hazardous or slippery road where the vehicles in the vicinity need to slow down or take further precautions,

(2) vehicle-to-infrastructure (V2I) warning such as car accidents or road sliding where the rescue teams (police or medical teams) can use the multimedia proof for an effective and timely response, (3) the last warning dissemination is the combination of the two scenarios. We do focus on the second scenario in this work and those files are called event-driven messages (EDM). Moreover, the EDM files would be sent to remote servers which will require a heavy bandwidth with excessive response delay. In big cities with millions of vehicles running on the road every day, the amount of data to be processed would be massive [2–4].

Edge computing was introduced as a new paradigm that takes the computing tasks to the network edge. The edge nodes collect data from the vehicles and process them rather than sending them to a central cloud server. This paradigm offers a number of benefits such as geo-distribution and low latency and can be applied in vehicular networks to offer real time services such as emergency warning, road surface monitoring and navigations [5–7]. However, despite the merits of edge computing in vehicular communications, the proposed solutions and applications have not been deployed worldwide due to lack of scalability and adequate communication supports. Recently, the researchers have raised the limitations of IEEE 802.11p due to its lacks of mobility support, also the long-term evolution (LTE) of fourth generation networks (4G) cannot offer effective latency that suits the vehicular networks based applications [8–10]. To overcome these limitations, 5G cellular networks were adopted as the ultimate architecture which could help a real deployment of vehicular based technologies. For instance, Uber made a successful test of driverless vehicle using 5G cellular networks recently. The cellular networks offer higher mobility support, reduced latency and massive connectivity that are core requirements for vehicular applications [11–13]. Meanwhile, security and privacy issues are also a considerable concern for vehicular communications. For example, vehicles reporting the emergency warnings might not need to disclose their locations expect to authorized third parties. The identities of the vehicles participating in the sending the warnings, their destinations and itinerary are highly sensitive information that need to be carefully handled. Currently, the misuse of vehicles' users data have been reported massively in the press where untrusted third parties and malicious users leaked the vehicles' sensitive data [14].

In the literature, a considerable number of articles has been published on secure message dissemination for vehicle networks and can be categorized in three groups: (1) Security for beacons messages also knows as basic safety message (BSM) for the US. These are periodic messages containing vehicle's position, speed and direction, etc. [15–17]; (2) event-driven message (EDM) that are generated at the time of occurrence such as accident alerts or emergency reports [18]. There are many solutions that addressed BSM based scenarios for privacy and security as shown in this recent survey [19]. However, these schemes cannot be directly applied to EDM scenarios for the following reasons. First, the schemes are not built based on 5G-enabled architecture which offers low latency and mobility support for vehicular communications. Second, the current literature such as [20] mainly suggests anonymous authentication schemes and message encryption for secure communications and the central cloud or edge nodes are mainly supposed to be secure. However, if the central cloud is compromised, the rescue services can not retrieve the important files needed for their services, thus data auditability and reliability is very crucial and one of the solutions to achieve data auditability would be through a private blockchain maintained by the edge devices [21,22]. Third, most of the schemes is built using expensive bilinear pairing techniques which are expensive and time consuming operations that degrade the overall protocol performance. To the best of our knowledge, there is one relevant article for emergency message dissemination for vehicular communications [23]. The authors basically presented a fog assisted architecture, highlighted limitations of relevant schemes in the literature and concluded with open research discussions.

Thus, a privacy preserving, secure yet auditable protocol for emergency message in vehicle edge computing is appealing. The contributions of this paper are three folds:

- We describe a novel architecture for emergency warning dissemination using edge computing and private blockchain. The proposed architectures uses 5G network technologies for communication.

In our model, we design a secure and privacy preserving model that protect the sensitive data (identity, location, shared data, etc) of the vehicles participating in emergency warning dissemination. We assume that the edge nodes and cloud are semi trusted, therefore our architecture proposes a private blockchain using edge nodes to record the EDM in an immutable and verifiable ledger to guarantee EDMs auditability.

- We design a secure and blockchain based EDM protocol for 5G enabled vehicle edge computing using the private blockchain technique to provide EDM auditability. We make use of lightweight multi-receiver signcryption scheme without pairing that offer low time consuming operations, security, privacy and access control.
- We provide an analysis of security and privacy features of the proposed protocol and evaluation in respect of private blockchain construction, computational and communication costs.

The remainder of this paper is as follows. We review the related work on 5G enabled vehicular edge computing and secure emergency message dissemination in Section 2. We design the system model and the preliminaries of the core cryptographic schemes used in our protocol in Section 3. Section 4 describes the proposed scheme and we provide security, privacy and performance analysis in Section 5. Finally, the concluding remarks are given in Section 6.

2. Related Work

This section first describes the basic concepts of vehicular edge computing, then outlines the basic notions of private blockchain technology and concludes with a review of the current schemes on EDM schemes in vehicular networks.

2.1. 5G Enabled Vehicular Edge Computing

Vehicular edge computing (VEC) or vehicular edge computing networks (VECONs) are extended from the conventional VANETs. The main difference is that VEC are made by an additional edge layer [24,25]. VEC is basically made by three layers, first the vehicle layer where the embedded sensors in the vehicle collect the data and send them to the edge layer using the onboard unit (OBU). The edge layer is a cluster made by several roadside units (RSUs) within a given distance. The RSU keeps or processes the data provided by the vehicles in the edge cluster. The following layer is called the cloud layer that manages the edge layers. The cloud layer can store massive data and make complex delay tolerant operations on the data provided by the edge layers. The cloud layer can be a data center or intelligent transportation system or regional trusted authority. Although 4G technology can be used, there are inherent drawbacks that has been raised by the research community for an effective vehicular communications networks using 4G technologies. A number of attacks performed on the international subscriber identity for the 4G LTE networks revealed its weakness to provide integrity, non-repudiation, accountability on user data. In addition, IEEE 802.11p can not be relied on for VEC due to its lack of mobility support [8–10]. In the forthcoming fifth-generation (5G) cellular-based vehicle networks, the use of denser and smaller cells are anticipated to offer a high transmission rate for the vehicles users. This will enable a range of application starting from the safety related applications to entertainment use cases. The nature of vehicular networks presents a different requirement from the conventional mobile networks. This is basically due to the volatile mobility of the vehicles in the network, the speed of the vehicles along with the topology of the dynamic wireless networks. Therefore, the use of 5G cooperative small cells is discussed in the literature as a promising recommendation [26–28]. We adopt in this paper a 5G enabled edge vehicular computing model as underlying network architecture for the proposed protocol.

2.2. Blockchain

Blockchain technology is a distributed ledger technique that was first introduced for the financial domain starting with Bitcoin crypto currency. It offers data auditability using authenticated blocks

added on the system. It is also a decentralized network since it does not require a centralized entity because it is a peer to peer network [21,22]. In order to add a new block, a consensus algorithm need to be agreed upon by the entities in the chain. Private blockchain was introduced for restricted environment such as businesses or companies where public readability can not be applied. A private blockchain is a network where the participants require a permission to join. In this work, we consider a proof of stake consensus algorithm that randomly choose one of the entities proportionally to each node's stake to run the process [29].

2.3. Secure Schemes for Emergency Warning in VEC

A considerable number of researchers have documented security and privacy related solutions for BSM based scenario as shown in this survey [18]. Nevertheless, these schemes are not directly applicable to EDM scenarios for the following reasons. The protocols do not consider a 5G-enabled architecture which offers low latency and mobility support for vehicular communications. Then, the schemes in the literature such as [20] mainly suggest anonymous authentication techniques and EDM/BSM encryption for secure communications while the central cloud or edge nodes are most of the time supposed to be secure. As mentioned earlier, this raises a huge issue with billions of connected devices, the regional or center cloud or edge devices can be compromised, thus data auditability and reliability need to be taken into consideration. One alternative way of achieving data auditability would be through a private blockchain maintained by the edge devices [21,22]. Also, most of the scheme such as [20] are built using expensive bilinear pairing techniques which are very heavy for mobile and ad hoc networks. In [23], the authors proposed an emergency message dissemination for vehicular communications. Though the paper specifically target EDM, the authors mainly presented fog assisted architecture, highlighted limitations of relevant schemes in the literature and concluded with open research discussions. Their protocol do not address security issues, latency sensitive architecture, distributed environment and EDM reliability and auditability. Thus, we are appealed in this paper to investigate on secure communication for EDM scenario taking into consideration that EDM could be very heavy (heavy videos, audio), while the privacy of the vehicles' users is not neglected, yet EDM reliability and auditability are guaranteed.

3. System Model

In this section we first present the system architecture of the proposed protocol and outline the basic concepts of cryptographic techniques used to construct our protocol.

3.1. Main Entities

Our proposed system model is made by a main regional overviewer called RTA, the road side units (RSCs) that make a edge cluster and the vehicles that provide EDM files collected through their sensors as shown in Figure 1. We outline the role of each entity in the following:

- Regional Transportation Authority (RTA): RTA is considered as a trusted agency that offers the registration of all the entities within the proposed system (vehicles and edge nodes) and generate cryptographic materials to the entities during the system setup.
- RSU edge nodes: Similar to a sever with limited capabilities, edge nodes are devices placed on the roads with efficient computing, communication and also storage aptitude. Their principal role is the collection of EDM provided by the vehicles, verifies the validity of EDM through designcryption and share the EDM to RTA or any entity that might need the EDM. In real life applications, the EDM could be needed by rescue services such as police or medical centers. We did not explicitly add these entities but we assumed that they have servers in the cloud which are connected to RTA servers as shown in Figure 1. We assume that edge nodes are connected to a source that generate electricity power.

- Vehicles: The vehicles are assumed to be equipped with several sensors and devices such as camera. The onboard units (OBU) in the vehicle gather all the those data in form of EDM files, sends them to edge nodes using different communication means such as D2D or mmWave communications. All vehicles need to register with the RTA at the time of periodic inspection. Besides the well known identifiers of vehicles such as the Electronic License Plate (ELP) or the electronic chassis number (ECN), every vehicle is given a 5G unique identifier (5GID), which is similar to subscriber identification module (SIM) as it is for 3G and 4G cellular networks.

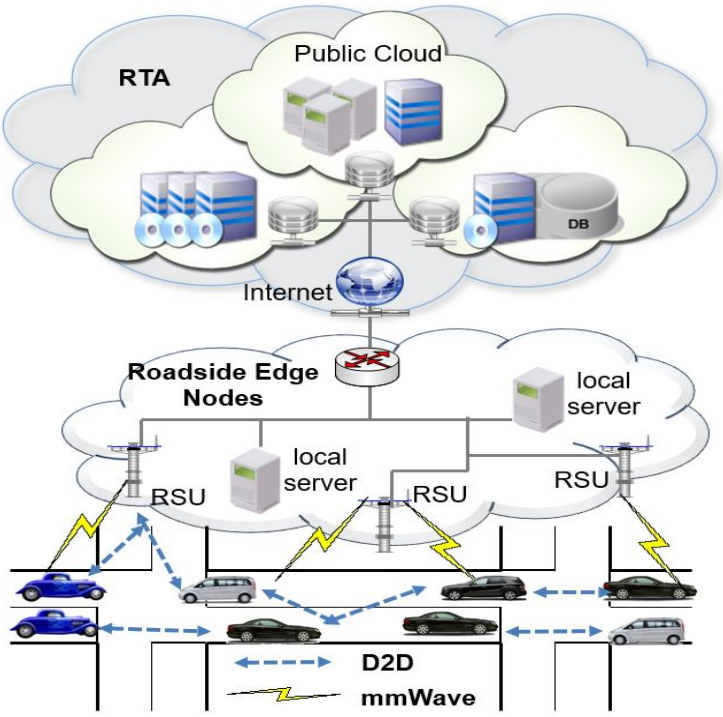


Figure 1. System architecture.

3.2. Communication Model

Motivated by the 5G cellular networks architecture, the proposed 5G enabled vehicle edge computing is made by the following components:

- Heterogeneous networks: This network aims at achieving high data rate and network capacity for the 5G-enabled vehicle edge computing. Therefore, two alternative techniques may help to get the mentioned capacities through smaller cells which increase the spectral efficiency. In addition, 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 [11].
- D2D Communications: D2D communication would enable the vehicles to communicate with each edge device within the licensed cellular bandwidth without considering the base stations. In the 5G edge based vehicular networks, the communication between the vehicles and edge devices can be done through D2D communication or mmWave technology.

3.3. Adversary Model

In this section, we describe the main attacks which an malicious user might conduct in the absence of this protocol EDM reporting scheme.

- A malicious vehicle can try to send EDM files when he is not enrolled for participation.
- A malicious user or vehicle can try to know the identity of the vehicles that reported the EDM file.

- A malicious vehicle can try to get the raw content of EDM which were sent through the network.
- A malicious vehicle can try to attack one or several edge nodes and try to process the EMD by impersonating a given edge node.
- A number of attackers (within or without the participating group) can try to jeopardize the whole network through a denial of service attack.

3.4. Security Objectives

We outline the security goals which the proposed scheme needs to achieve:

- Identity privacy preservation: the identities of the vehicles that report the EDMs should be preserved.
- Authentication: each vehicle that is involved in sending the EDMs should be authenticated before it is allowed to join the system.
- Confidentiality and integrity: the EDMs files generated and sent through the network should not be intercepted and modified during the communication.
- Key escrow resilience: the keys of the entities (vehicles) participating in EDM reporting should not be generated by a single entity. Thus, even if the RTA is comprised, the attackers can not disclose the signing keys of the vehicles.
- Access control: only the entities with matching policies should be able to retrieve the contents of EDMs.
- Non-repudiation and traceability: a vehicle should not deny any participation in the EDM reporting. In addition, RTA should be able to disclose the true identity of any entity if needed.
- Auditability: the EDMs records that are saved in the system should be securely kept and easily verifiable. Even if one node in the chain is compromised, the malicious user should not be able to modify and upload any EDM content.

3.5. Preliminaries

In this section, we describe the two main cryptographic techniques used to build our protocol. We first outline a lightweight signcrpytion technique which is not built on pairing operations, we also describe the underlying concepts for constructing a private blockchain.

3.5.1. Signcryption Scheme without Bilinear Pairings

This scheme is made by six sub protocol namely Setup, SecretValue, Partialkeypair, keypair, Signcryption and DeSigncryption [30].

- $Setup(1^{\lambda})$: using a parameter λ, RTA runs the system to generate a master secret key mk and the parameters $params$.
- $SecretValue(ID, params)$: a user runs the algorithm to return a secret value V_{ID} using his/her identity ID.
- $Partialkeypair(params, V_{ID}, ID)$: RTA runs the algorithm and returns the partial private key y_{ID} and partial public key D_{ID} using the user identity ID and the secret value V_{ID}
- $Keypair(D_{ID}, y_{ID}, params)$: the user generates the key pairs (PK_i, SK_i) using the partial key pairs (D_{ID}, y_{ID}).
- $Signcrypt(L, m, SK_i, params)$: the user target a group of authorized receivers' public keys $L = \{PK_1, PK_2, PK_3, .., PK_n\}$ where n is a positive integer. Output a ciphertext δ on the message m.
- $Designcrypt(params, \delta, SK_i)$: using the system parameters $params$, the receiver's private key SK_i and the ciphertext δ, an authorized receiver recovers the message m.

3.5.2. Private Blockchain

The private blockchain concept used in the paper is made by the following sub-phases, namely setup, initial stage, leader selection and block generation [21,22]:

- Setup: in this phase, different slot $\{ts_1, ts_2, ts_3, \cdots\}$ are generated and a private ledger is attached with a one block for every time slot ts_i. In addition, a leader selection algorithm $F(.)$ is assigned to each edge node.
- Initial stage: this is a first stake distribution phase when the first block also called genesis block is generated. The genesis block includes the edge nodes identities, public keys and stakes. The first block is assumed to have an empty blockheader and signcryption is generated on it.
- Leader selection: taking each time slot ts_i, the edge nodes identities, their public key, the probability of an edge node corresponding to its stake, this function output the node leader.
- Blockgeneration: the chosen leader generates a new block which is made by a block header, its stake, the number of EDM recorded. Note that the blockheader is made by a blockheader number, hash of previous blockheader, a merkle hash root along with a time stamp. For interested readers, the overall details can be found in [21,22].

4. Protocol Description

Our proposed protocol is made by five main sub-protocols: setup, participation agreement, EDM reporting, EDM collection and private blockchain generation

4.1. Protocol Setup

Our protocol assume that a regional traffic authority (RTA) manages the reporting of EDM messages, therefore both the vehicles and the edge nodes in the region are registered to the RTA. *RTA* first runs $Setup(1^{\lambda})$ to generates the parameters parameters $(\mathbb{G}_1, q, P)$ with the $\mathbb{G}_1$ being a cyclic additive group of order q and a generator P over an elleptic curve that is defined on finite field F_w where w is an integer chosen by RTA. *RTA* then selects a random $s \in \mathbb{Z}_q^*$ as a master secret and generates the public key of *RTA* as $P_{RTA} = sP$. *RTA* selects five hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$, $H_2 : \{0,1\}^* \rightarrow \mathbb{G}_1$, $H_3 : \{0,1\}^* \rightarrow \mathbb{G}_1$, $H_4 : \{0,1\}^* \rightarrow \mathbb{G}_1$, $H_5 : \{0,1\}^* \rightarrow \mathbb{G}_1$ and publishes the public parameters $(\mathbb{G}_1, H_1, H_2, H_3, H_4, H_5, P_{RTA}, P, q)$ to all the entities.

4.2. Participation Agreement

In order to participate in EDM reporting, the vehicles and the edge nodes are registered by the RTA. The registration of these entities is done as follows

- Step 1. Assume there is a vehicle inspection within a given period (12 or 18 months), the vehicle owner or user can express its desire to be part of EDM reporters. In this case, the vehicles does the following:

  1. A vehicle v_i with its identity $5GID_{v_i}$ selects a secret $t_i \in \mathbb{Z}_q^*$ and computes $V_{v_i} = t_1 P$ and send $(5GID_{v_i}, V_{v_i})$ to *RTA*.
  2. Upon receiving $(5GID_{v_i}, V_{v_i})$, *RTA* choose a pseudonym for $5GID_{v_i}$ as $P5GID_{v_i}$, and keep the mapping table securely. *RTA* selects $d_i \in \mathbb{Z}_q^*$ and computes $y_i = H_1(P5GID_{v_i}, V_{v_i}, d_i) + s(mod)w$ and $D_i = H_1(P5GID_{v_i}, V_{v_i}, d_i)P$. Then *RTA* returns (D_i, y_i) to v_i
  3. v_i receives (D_i, y_i) and checks if the equation $y_i P = D_i + P_{RTA}$ is correct. If yes, v_i generates its public key $PK_{v_i} = D_i + H_2(P5GID_{v_i}, V_{v_i})V_{v_i}$.
  4. v_i generates its private key $SK_{v_i} = H_2(P5GID_{v_i}, PK_{v_i})(y_i + H_2(5GID_{v_i}, V_{v_i})t_i)(mod)w$. The key pair of the vehicle v_i is (PK_{v_i}, SK_{v_i}).

- Step 2. In the same way, *RTA* registers the edge nodes as follows:

1. A edge node Ed_i with its identity ID_{Ed_i} selects a secret $m_i \in \mathbb{Z}_q^*$ and computes $V_{Ed_i} = m_1 P$ and send (ID_{Ed_i}, V_{Ed_i}) to RTA.
2. After receiving $(5GID_{Ed_i}, V_{Ed_i})$, RTA selects $f_i \in \mathbb{Z}_q^*$ and computes $a_i = H_1(ID_{Ed_i}, V_{Ed_i}, f_i) + s(mod)w$ and $F_i = H_1(ID_{Ed_i}, V_{Ed_i}, f_i)P$. Then RTA returns (F_i, a_i) to v_i
3. Ed_i receives (F_i, a_i) and check if the equation $a_i P = F_i + P_{RTA}$ is correct. If yes, Ed_i generates its public key $PK_{Ed_i} = F_i + H_2(ID_{Ed_i}, V_{Ed_i})V_{Ed_i}$.
4. Ed_i generates its private key $SK_{Ed_i} = H_2(ID_{Ed_i}, PK_{Ed_i})(a_i + H_2(ID_{Ed_i}, V_{Ed_i})m_i)(mod)w$. The key pair of the edge node Ed_i is (PK_{Ed_i}, SK_{Ed_i}).

4.3. Emergency Driven Message Reporting

Whenever an emergency event such as land sliding occurs, v_i performs the following:

- Composes EMD file as $M = \{Dt, Ts, loc, file\}$ representing the date, the time, the location and main file which has been captured. $file$ could be a multimedia item such as pictures or audio files.
- v_i generates a list of edge nodes that can recover the message, and in this case we adopt proximity protocol based on the location as described in [31]. v_i generates $L = \{ID_{Ed_1}, ID_{Ed_2}, ID_{Ed_3}, \cdots, ID_{Ed_n}\}$ and make the signcryption on the event message as follows

1. Computes $Q_i = PK_{Ed_i} + P_{RTA}$ with $i = 1, 2, 3, \cdots, n$
2. Selects a integer $x \in \mathbb{Z}_q^*$ and computes $X = xP$ and $C_i = xH_2(PID_{Ed_i}, PK_{Ed_i})Q_i$ and $\alpha_i = H_3(C_i, X)$ where $i = 1, 2, ..n$
3. Selects an integer $\xi \in \mathbb{Z}_q^*$ and computes the polynomial $f(v) = \prod_{i=1}^{n}(v - \alpha_i) + \xi(mod)w$, which equals to $a_0 + a_i v + .. + a_{n-1}v^{n-1}$ for $a_1 \in \mathbb{Z}_q^*$
4. Computes $k = H_4(\xi)$, $J = Enc_k(m||P5GID_{v_i})$ and $h = H_5(m||P5GID_{v_i}, \xi, a_0, a_1, .., a_{n-1}, X)$
5. Generates h^{-1} that satisfy $hh^{-1} \equiv 1(mod)w$ and computes $z = h^{-1}(SK_{v_i} + x)(mod)w$
6. Generates the cipher text $CT =< J, X, z, h, a_0, a_1, \cdots, a_{n-1} >$ and send it to edge nodes.

4.4. Emergency-Driven Message Collection

Upon receiving the cipher text CT, an edge node Ed_i does the following to recover the emergency warning

- Compute $C_i = SK_{Ed_i}X$ and $\alpha = H_3(C_i, X)$
- Then computes $f(v) = a_0 + a_i v + .. + a_{n-1}v^{n-1} + v^n$ and $\xi = f(\alpha_i)$
- Computes $k = H_4(\xi)$ and retrieve the message trough the decryption $Dec_k(J) = m||P5GID_{v_i}$
- Also compute $h^{'} = H_5(P5GID_{v_i}, \xi, a_0, \cdots, a_{n-1}, X)$ and verifies if the equation $h = h^{'}$ is correct. Otherwise, the emergency message is rejected
- Upon receiving the vehicle public PK_{v_i},Ed_i checks if the equation $hzP = H_2(P5GID_{v_i}, PK_{v_i})(PK_{v_i} + P_{RTA})$. The correctness is as follows:

$$
\begin{aligned}
&= hh^{-1}(SK_{v_i} + x)P \\
&= SK_{v_i}P + W \\
&= H_2(P5GID_{v_i}, PK_{v_i})(y_i + H_2(P5GID_{v_i}, V_{v_i})t_i)P + X \\
&= H_2(P5GID_{v_i}, PK_{v_i})(D_i + H_2(P5GID_{v_i}, V_{v_i})V_{v_i} + P_{RTA}) + X \\
&= H_2(P5GID_{v_i}, PK_{v_i})(PK_{v_i} + P_{RTA}).
\end{aligned}
$$

If yes, Ed_i keeps the EDM message.

4.5. Private Blockchain Generation

We do assume that every edge node Ed_i is a stakeholder having its proper stake that could be the number of valid EDM that Ed_i has received. A private blockchain $Chain$ is constructed as follows:

1. Assume that the time is divided into time slot $\{ts_1, ts_2, \cdots, ts_1\}$ in which a block is attached to the ledger for each time sequence.
2. The initial block also called genesis block is generated as the first state distribution and it contains the edge nodes identities, their public keys, their stakes as $B_{gen} =< \{\mathrm{ID}_{Edi=1}{}^{R}\}, \{PK_{Ed}\}_{i=1}^{R}$ and $\{ST_{Ed}\}_{i=1}^{R} >$. We assume that first blockheader B_{gen} to be empty.
3. Therefore, in a given area, each edge node Ed_i set $C = B_0$ where B_0 is the genesis block
4. An edge node Ed_i collects n EDM and verifies each EDM as shown in Section 4.4 by running $Designcrypt(params, \delta, SK_i)$. To choose a leader edge node L_{Ed_i}, the probability p_i for being chosen should be relative to its stake that are in previous block.
5. Ed_i runs a leader selection protocol $F(.)$ [32] that input $< \{ID_{Edi=1}{}^{R}\}, \{PK_{Ed}\}_{i=1}^{R}, p_{Ed_i}, st_i >$ representing respectively the edge nodes identities, their public key, the probability of the leader and the corresponding time slot with $p_{Ed_i} = st_i / \sum_{j=1}^{Ed_i} st_{Ed_i}$.
6. $F(.)$ outputs a leader edge node $L_{Ed_i} \in \{Ed_i, Ed_2, Ed_3, \cdots, Ed_n\}$
7. To generate a block, the selected edge node L_Ed_i output a block B_{ts_i} that corresponds to the time slot ts_i with $B_{ts_i} = \{Num_{ts_i}, H_{ts_i}, MHR_{ts_i}, t_{ts_i}\}$ representing respectively the number of the block, a hash corresponding to previous blockheader, merkle hash root corresponding to a merkle tree built using n EDM.
8. Ed_i performs the update of its stake st_{ts_i} and generates a signcryption on the entire message.
9. Finally add the block to the chain and send a notification to the entire network

5. Performance

This section is made by the security analysis of the proposed protocol, the experiment on private blockchain, the computational and communication cost along with the simulation.

5.1. Security Analysis

We provide in this section the analysis in regards to the security goals for the proposed scheme.

5.1.1. Privacy Preservation

The communication within the proposed protocol is entirely based on anonymous interactions. While the vehicles engaged in reporting EDM are sending their messages, they make use of pseudonyms. RTA is the one and only entity that can map the real identity of a vehicle participating in the EDM reporting to its pseudonyms. As described in Section 4, when v_i requests partial key pair by running the function $Partialkeypair(params, V_{ID}, ID)$, it sends its real identity to RTA which generates a pseudonymous $P5GID_{v_i}$. Therefore it is infeasible for any entity inside or outside the network to know the real identity of the EDM participant except the RTA. This would require the adversary to access the database that maps the vehicles real identities and their pseudonyms.

5.1.2. Authentication

In the proposed protocol, bad actors or malicious vehicles or any entity can not successfully engage in forging an EDM report because the authentication between a vehicle v_i and an edge node Ed_i is achieved through the signcryption function $Signcrypt(L, m, SK_i, params)$ that is made on each message. Once an EDM is generated, v_i makes signcryption of the message $M = \{Dt, Ts, loc, file\}$ by running $Signcrypt(L, m, SK_i, params)$. Any entity needs to possess a valid private key SK_i to be able to verify the correctness of the equation $hzP = H_2(P5GID_{v_i}, PK_{v_i})(PK_{v_i} + P_{RTA})$. It is hard for an adversary to have the full private key of an edge node because it is partial generated both by the RTA and the edge node through the functions $Partialkeypair(params, V_{ID}, ID)$ and $Keypair(D_{ID}, y_{ID}, params)$. The signcryption technique that was used to build the proposed protocol achieves unforgeability through the strong existential unforgeability against chosen plain text,selvi2008efficient. Therefore, we confirm that the proposed protocol achieves authentication property.

5.1.3. Confidentiality and Integrity

The proposed protocol achieves the confidentiality and integrity of the EDM messages that are sent by the vehicles to edge nodes through the two in one technique that both provide encryption and digital signature in a single step. As shown in Section 4, the cipher $CT =< J, X, z, h, a_0, a_1, \cdots, a_{n-1} >$ accomplishes the duties of message encryption and signature. A malicious user can not tamper with the integrity of the EDM because the signcryption phase transform the data into hash values $C_i = xH_2(PID_{Ed_i}, PK_{Ed_i})Q_i$ and $\alpha_i = H_3(C_i, X)$ as described in Section 4. Thus, we guarantee that the proposed scheme achieves data integrity and confidentiality because the underlying technique is fully proved to satisfy security under adaptively chosen ciphertext [33].

5.1.4. Key Escrow Resilience

The 4th industrial revolution projects a massive connectivity of devices to offer diversified services such as EDM reporting using the inbuilt vehicle sensors. In additional, 5G cellular networks were adopted in this work to provide effective latency. Security wise, key escrow resilience property needs to be achieved for applications within a massive connectivity environment. In the proposed scheme, the entities first generate a secret value by running $SecretValue(ID, params)$ and RTA will then provide partialkey pair to the entities by computing $Partialkeypair(params, V_{ID}, ID)$ function. The entities in our system compute their key pairs through the function $Keypair(D_{ID}, y_{ID}, params)$. Therefore, the proposed protocol achieves key escrow resilience.

5.1.5. Access Control

In the current era with millions of devices connection, a single point failure should be avoided as much as possible. While the EDM are categorized to be safety related messages that contain sensitive data, multi receiver property (or access control) is a key point that need to be considered. In the proposed protocol, a vehicle v_i selects a number of valid edge nodes, in this case, even in a scenario where a number of edge nodes have been compromised, the probability that the EDMs at least get to one receiver is higher. Therefore v_i generates $L = \{ID_{Ed_1}, ID_{Ed_2}, ID_{Ed_3}, \cdots, ID_{Ed_n}\}$ and run $Signcrypt(L, m, SK_i, params)$ to signcrypt the messages. Only valid receiver within the L can recover the EDM. Therefore, the proposed scheme achieves fine-grained access control by using attribute based encryption.

5.1.6. Traceability and Non Repudiation

In the proposed system, when a valid user sends a fake EDM (probably for criminal profit), the edge node will discard the message because the signcryption correctness $hzP = H_2(P5GID_{v_i}, PK_{v_i})(PK_{v_i} + P_{RTA})$ will not hold. However, Ed_i will keep a log of pseudo identity of the vehicles. Thus, the vehicle can not deny its own pseudo identity. Additionally, in case of legal disputes, RTA consults its database that maps the identities and their pseudo identities to reveal the real identity of the vehicle. Therefore, we do confirm that the proposed protocol can achieve traceability and non repudiation of misbehaving entities.

5.1.7. Auditability

The proposed scheme does achieve data auditability by building a private blockchain between the edges nodes. The achievement of this property can be summarized in three steps:

- The blockchain that is built in this scheme is private, any participant requires a permission or an invitation to join the private chain. In this case, it is infeasible for an malicious user to add bogus block to the chain.
- Each participant in the private chain keeps a replica of any appended ledger of emergency warning messages. This is crucial in case a crash occurs in any of the remote servers where the EDM are kept.

- Transactions immutability: It is hard for a malicious entity to tamper the EDM that is exchanged between the vehicles and the edges. In case of a legal dispute that require the thorough auditability of the EDM, the transaction immutability of blockchain can strengthen such services.

5.1.8. Secure against Known Attacks

We describe in this section few well known attacks within the vehicular networks and how our proposed scheme can overcome them.

- Impersonation attack: as mentioned earlier, the malicious vehicles cannot succeed to impersonate a legitimate vehicle because the authentication between a vehicle v_i and an edge node Ed_i is achieved through the signcryption function $Signcrypt(L, m, SK_i, params)$ that is made on each message. Once an EDM is generated, v_i makes signcryption of the message $M = \{Dt, Ts, loc, file\}$ by running $Signcrypt(L, m, SK_i, params)$. Every participating vehicle needs to possess a valid private key SK_i to be able to verify the correctness of the equation $hzP = H_2(P5GID_{v_i}, PK_{v_i})(PK_{v_i} + P_{RTA})$. Based on the hardness of the DL problem, the signature provided on the message cannot match the verification and the message will be discarded. Thus, it is almost impossible to perform an impersonation attack in our proposed scheme
- Masquerade attack: suppose a malicious user eavesdrops an EDM message and tries to know the EMD contents. That malicious user can not tamper with the integrity of the EDM because the signcryption phase transforms the data into hash values $C_i = xH_2(PID_{Ed_i}, PK_{Ed_i})Q_i$ and $\alpha_i = H_3(C_i, X)$ as described in Section 4. Therefore, the malicious user cannot learn any useful information from the eavesdropped message nor reveal the identity of the message owner.
- DDoS attack: our scheme is able to resist against DDoS attacks either launched by legitimate or illegitimate vehicles. Assume an illegitimate vehicle tries to send multiple EDM to a given edge node, as demonstrated in the impersonation attack, those EDM will be discarded by the edge node because the message verification will not hold. In addition, assume a legitimate vehicle is generating excessive EDM to cause a DDoS attack, in that scenario, the edge nodes will use the time stamp on any EDM given message to predict the frequency of message compared to other users because every EDM message contains a time stamp as shown in message content as $M = \{Dt, Ts, loc, file\}$ representing respectively the date, the time, the location and $file$ which could be a multimedia item such as pictures or audio files. Therefore, the messages from the suspicious user can be discarded.

5.2. Computational Cost

In this section we provide the analysis of the proposed protocol in terms of generating the EDM by the vehicle and the recovery of the message by the dedicated node. We performed the benchmark using a desktop of Core i7 3.5-GHz,16GB RAM with a crypto ++ library [34] with 6 as the embedded degree and $\mathbb{G}$ and q equivalent respectively to 161 bits and 160 bits. We mainly focused on the following main operations; point scalar multiplication, modular exponentiation and bilinear pairing. These operations dominate the process of sending and receiving the emergency messages. Table 1 shows the cost of the main cryptographic operations. A vehicle v_i after generating the EDM, it performs $(T + 1)T_m + nT_p$ to signcrypt a emergency message while the designcrypt operation requires $2T_m + T_p$ as shown in Table 2. As mentioned, there are several articles that addressed security solutions for BSM messages but few have addressed the EDM. BSM content being a predefined with limited content, the size of the BSM is supposed to be small and constant. As shown in this recent survey on secure protocol for vehicular communications [19], we compared the proposed protocol with the protocol in [20] as shown in Table 3.

We further considered two main elements than can effect the complexity of the whole scheme. First we investigated the number of attributes that can be associated with a given policy. Assume a user v_i wants to share his emergency files with five governmental agencies. For instance, the emergency

files contains few pictures of a land sliding scene. Those pictures can both be used by the ambulance team, the evacuation, the police and any other. Therefore the access policy might contain a number of attributes. In our simulation scenario we considered a range of attributes varying from 0 or 50, $range = [0 - 50]$. We then investigate the time needed for signcryption and designcryption based on the number of attributes in a given access policy. It is obvious that the obtained results are increasing gradually based on the number of attributes. For an average number of 30 attributes, the designcryption time was 17 s as shown in Figure 2a. Though the results are not very competitive, they are still feasible especially for edge nodes that have considerable computing capabilities. Also, we investigated the time needed for signcryption and designcryption when the number of files is fixed. The cost of encryption for one of two files was constant since we assume that the files (assume three separate images taken from different angles) are encrypted using a similar access policy. On the other hand, the decryption phase took much more time due to reconstruction of the secret value using Lagrange algorithm. As shown in Figure 2b, for a maximum folder of 10 files, we have a decryption cost of around 32 s. Since the decrypting devices could be servers or computing gadgets with sufficient communication power, the obtained decryption is acceptable for non real-time scenarios such as EDM reporting.

Table 1. Measurement of cryptographic operations.

Notation	**Operations**	**Time (ms)**
T_b	Bilinear pairing	4.5
T_m	Point scalar multiplication	0.6
T_p	Point adddition on ECC	0.047
T_e	Exponentiation	3.9
T_{as-dec}	Asymmetric decryption	0.61
T_{s-enc}	Symmetric encryption	0.51
T_{s-dec}	Symmetric decryption	0.55
T_h	Execution time of a general hash function	0.0001

Table 2. Computational cost of signcrypt and designcript (n is number of receiver).

Phase	**Operation**
Signcryp an EDM	$(T+1)T_m + nT_p$
Designcryp an EDM	$2T_m + T_p$

Table 3. Comparison Performance of Proposed Work and literature.

Scheme	**lightweight**	**Traceability**	**Tamper Proof**	**Privacy**	**Decentralization**	**IoT Friendly**
Liu et al., [20]	Low	YES	Low	Yes	NO	NO
Proposed Framework	High	YES	HIGH	YES	HIGH	HIGH

There are a considerable number of schemes within [19], however, these protocols are built based on expensive operations that compromise their efficient even if these protocols address BSM scenarios. For EDM, the size can be very important with the multimedia contents that can be added, thus a lightweight protocol could be more efficient. In additional, the protocols in the survey are not decentralized to offer immutability of transactions, however we achieve this property in our scheme by using private blockchain.

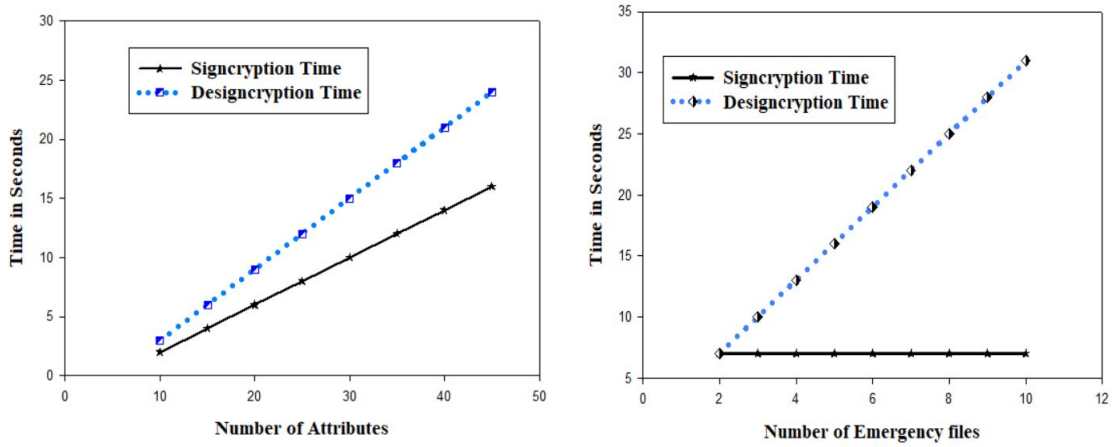


Figure 2. Signcryption/Designcryption time versus Number of Attributes (**a**) and Signcryption/Designcryption time versus Number Emergency Files (**b**).

5.3. Communication Cost

In this section, we provide the communication cost of the proposed protocol. We first computed the overhead caused by the additional cryptographic primitives that were added on the raw message. We did not consider the element in the EDM since this can vary in real life application based on the multimedia content within an EDM. As mentioned in [35], in pairing operations, the size of elements equals to $64 \times 2 = 128$ bytes while for the ECC based operations, the size of the elements are equal to $20 \times 2 = 40$ bytes. As seen in the construction of the proposed, our scheme is not built based on pairing operations, and as described in Table 2, the size caused by security primitives are 80 bytes for the proposed protocol.

5.4. Private Blockchain Evaluation

We perform the experiments for the private blockchain that was built based on the edges nodes. Our experiment considers seven settings. As shown in Table 4, we considered a scenario that can generate 5 to 35 blocks. In the three first settings, we assumed 10 edge nodes while we considered 15 edges nodes in the four last settings. We computed the average time within our seven steps including the time required from system setup to the generation of the block. As seen in Table 4, the additional cost caused by the generation of block is not very heavy for a 5G cellular network, in the same time this technique offers immutable transactions with EDM auditability even if one or several edge nodes crash. We can see from the table that an edge node can create a new block to the added on the private blockchain with a cost of 0.056 s during the seventh step.

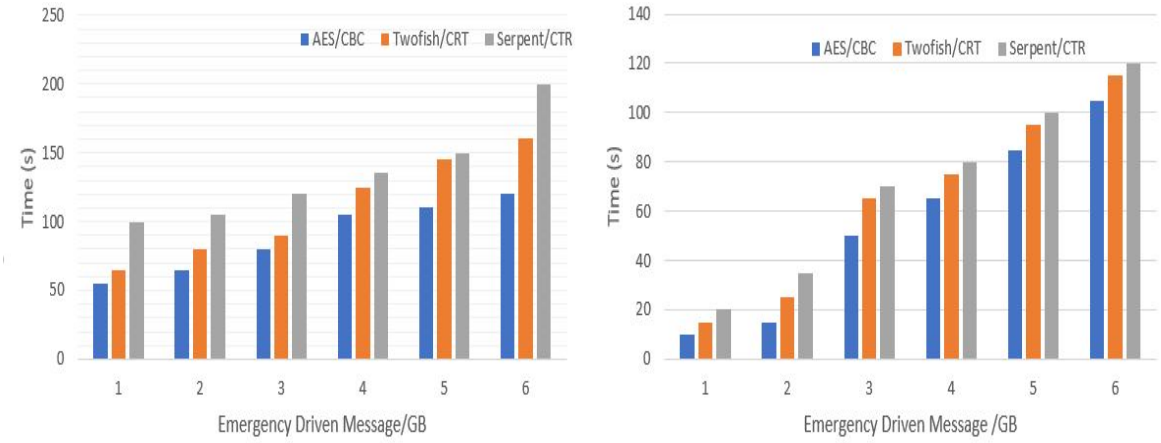
Table 4. Analysis of Edge node made private blockchain (/second).

Phase	No Trans/Block	No of ED	Initialization	Request	Response	Matching	Updating
1	5	10	0.022	0.44	0.15	1.89	0.0022
2	10	10	0.022	0.61	0.26	2.56	0.0089
3	15	10	0.022	0.98	0.63	2.29	0.014
4	20	15	0.045	1.44	0.89	3.51	0.031
5	25	15	0.045	1.79	1.25	4.01	0.056
6	30	15	0.045	2.14	1.67	4.98	0.17
7	35	15	0.045	4.12	3.90	6.67	0.56

5.5. Simulation

In this section we provide the simulation that focus on the network performance of the proposed protocol. To achieve this, we made use of VANETSIM 2.02 that offers simulation for vehicle mobility and NS-3 was considered as a tool for network simulation. In our simulation, we considered a 5G functional network that can achieve a connection speed of 1.2Gb/s as reported and confirmed in several reports [36]. We focused on analyzing the performance of well known block ciphers techniques that vehicles can choose as symmetric encryption k as shown in Section 4. These algorithms were TWOFISH/CTR with 256 bit key and speed of 147 MB/s, then SERPENT/CTR that has 256 bit key with a 65 MB/s speed and lastly the famous AES/CBC of 256 bit key for a 455 MB/s as speed.

The rest of the parameters that were considered in our simulation are described in Table 5. Our simulation mainly focus on the size of the EDM because till now we cannot tell what would be the real size of EDM, therefore using a 5G benchmarked connection, we investigated the performance of signcryption of EDM based on different sizes. The size of an EDM message varies between 1 to 6 Gigabytes. Figure 3b shows that the time needed by a vehicle to signcrypt an EDM, ranges between 20 to 40 s for an EDM that has a size of 2 GB. In addition, we investigated the overall time to signcrypt and designcrypt an EMD as shown in Figure 3a, we still found that as long as an EDM does not go beyond 2 GB of size, the overall time is not that much when we consider the 5G projected features. In this case, the highest record which corresponds to Serpent/CTR algorithm is around 100 s.



(**a**) (**b**)

Figure 3. Overall time overhead (**a**) and signcryption time overhead (**b**).

Table 5. Setting of simulation parameters.

Tools/Parameter	Value/Specification
Mobility generation tool	VANETSIM 2.02
Network Simulation tool	ns-3
Data Rate	1.2 GBps
Number-of-vehicle	200
Number-of-edge nodes	40
Distance between two edge nodes	150 m
Simulation time	100 min
Wireless protocol	802.11a
Departure interval	180 s
RSU/Edge radius	800 m
mobility model	shortest path
Range of EDM size	(1–6 GB)

6. Conclusions

In this paper, we presented a secure and blockchain based EDM protocol for 5G-enabled vehicular edge computing. To provide scalability and latency for the proposed scheme, we adopted a 5G cellular architecture due to its projected features compared to 4G long-term evaluation (LTE) for vehicular communications. We considered an edge computing architecture to provide local processing of EDM in order to improve the response time. We made use of lightweight multi-receiver signcryption scheme without pairing that offers lightweight consuming operations, security, privacy and access control. To keep EDM records into a distributed system for reliability and auditability, we constructed a private blockchain using the edge nodes. The performance analysis of the proposed protocol in terms of security analysis, communication, computational and simulation confirms the efficiency of the protocol.

Author Contributions: Conceptualization, L.N.; methodology, L.N.; validation, B.A.T.; writing—original draft preparation, L.N.; writing—review and editing, M.K.S.; supervision, Y.-H.C.; funding acquisition, Y.-H.C. All authors have read and agree to the published version of the manuscript.

Funding: This work was supported by BK21PLUS, Creative Human Resource Development Program for IT Convergence, by basic science research program through national research foundation korea (NRF) funded by the ministry of science, ICT and future planning (NRF-2018R1D1A3B07043392).

Acknowledgments: This work was supported by BK21PLUS, Creative Human Resource Development Program for IT Convergence, by basic science research program through national research foundation korea (NRF) funded by the ministry of science, ICT and future planning (NRF-2018R1D1A3B07043392).

Conflicts of Interest: Authors declare that there is no conflict of interest.

References

1. Sanguesa, J.A.; Fogue, M.; Garrido, P.; Martinez, F.J.; Cano, J.C.; Calafate, C.T. A survey and comparative study of broadcast warning message dissemination schemes for VANETs. *Mob. Inf. Syst.* **2016**, *2016*, 8714142.
2. Karagiannis, G.; Altintas, O.; Ekici, E.; Heijenk, G.; Jarupan, B.; Lin, K.; Weil, T. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE Commun. Surv. Tutorials* **2011**, *13*, 584–616.
3. Kamouch, A.; Chaoub, A.; Guennoun, Z. Mobile big data in vehicular networks: The road to internet of vehicles. In *Mobile Big Data*; Springer: Cham, Switzerland, 2018; pp. 129–143.
4. Nkenyereye, L.; Park, Y.; Rhee, K.H. Secure vehicle traffic data dissemination and analysis protocol in vehicular cloud computing. *J. Supercomput.* **2018**, *74*, 1024–1044.
5. Lavanya, R. Fog Computing and Its Role in the Internet of Things. In *Advancing Consumer-Centric Fog Computing Architectures*; IGI Global: Hershey, PA, USA, 2019; pp. 63–71.
6. Nkenyereye, L.; Liu, C.H.; Song, J. Towards secure and privacy preserving collision avoidance system in 5G fog based Internet of Vehicles. *Future Gener. Comput. Syst.* **2019**, *95*, 488–499.
7. Yi, S.; Li, C.; Li, Q. A survey of fog computing: Concepts, applications and issues. In Proceedings of the 2015 Workshop on Mobile Big Data, Hangzhou, China, 21 June 2015, pp. 37–42.
8. Mir, Z.H.; Filali, F. LTE and IEEE 802.11 p for vehicular networking: A performance evaluation. *EURASIP J. Wirel. Commun. Netw.* **2014**, *2014*, 89.
9. Vinel, A. 3GPP LTE versus IEEE 802.11 p/WAVE: Which technology is able to support cooperative vehicular safety applications? *IEEE Wirel. Commun. Lett.* **2012**, *1*, 125–128.
10. Bellalta, B.; Belyaev, E.; Jonsson, M.; Vinel, A. Performance evaluation of IEEE 802.11 p-enabled vehicular video surveillance system. *IEEE Commun. Lett.* **2014**, *18*, 708–711.
11. Shen, X. Device-to-device communication in 5G cellular networks. *IEEE Netw.* **2015**, *29*, 2–3.
12. Tehrani, M.N.; Uysal, M.; Yanikomeroglu, H. Device-to-device communication in 5G cellular networks: Challenges, solutions, and future directions. *IEEE Commun. Mag.* **2014**, *52*, 86–92.
13. Schneider, P.; Horn, G. Towards 5G security. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 20–22 August 2015; Volume 1, pp. 1165–1170.

14. Park, J.; Kim, J.; Lee, B. Are uber really to blame for sexual assault?: Evidence from New York city. In Proceedings of the 18th Annual International Conference On Electronic Commerce: e-Commerce in Smart Connected World, Suwon, Korea, 17–19 August 2016; p. 12.
15. Darus, M.Y.; Bakar, K.A. Review of Congestion Control Algorithm for Event-Driven Safety Messages in Vehicular Networks. *Int. J. Comput. Sci. Issues* **2011**, *8*, 49.
16. Djahel, S.; Ghamri-Doudane, Y. A robust congestion control scheme for fast and reliable dissemination of safety messages in VANETs. In Proceedings of the 2012 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, China, 1–4 April 2012; pp. 2264–2269.
17. Zhang, W.; Festag, A.; Baldessari, R.; Le, L. Congestion control for safety messages in VANETs: Concepts and framework. In Proceedings of the 2008 8th International Conference on ITS Telecommunications, Phuket, Thailand, 24 October 2008; pp. 199–203.
18. Ma, X.; Kanelopoulos, G.; Trivedi, K.S. Application-level scheme to enhance VANET event-driven multi-hop safety-related services. In Proceedings of the 2017 international conference on computing, networking and communications (ICNC), Santa Clara, CA, USA, 26–29 January 2017; pp. 860–864.
19. Ali, I.; Hassan, A.; Li, F. Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey. *Veh. Commun.* **2019**, *16*, 45–61.
20. Liu, Y.; Wang, L.; Chen, H.H. Message authentication using proxy vehicles in vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **2015**, *64*, 3697–3710.
21. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 839–858.
22. Gao, F.; Zhu, L.; Shen, M.; Sharif, K.; Wan, Z.; Ren, K. A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. *IEEE Netw.* **2018**, *32*, 184–192.
23. Ullah, A.; Yaqoob, S.; Imran, M.; Ning, H. Emergency message dissemination schemes based on congestion avoidance in VANET and vehicular FoG computing. *IEEE Access* **2019**, *7*, 1570–1585.
24. Zhang, K.; Mao, Y.; Leng, S.; He, Y.; Zhang, Y. Mobile-edge computing for vehicular networks: A promising network paradigm with predictive off-loading. *IEEE Veh. Technol. Mag.* **2017**, *12*, 36–44.
25. Feng, J.; Liu, Z.; Wu, C.; Ji, Y. AVE: Autonomous vehicular edge computing framework with ACO-based scheduling. *IEEE Trans. Veh. Technol.* **2017**, *66*, 10660–10675.
26. Wang, C.X.; Haider, F.; Gao, X.; You, X.H.; Yang, Y.; Yuan, D.; Aggoune, H.M.; Haas, H.; Fletcher, S.; Hepsaydir, E. Cellular architecture and key technologies for 5G wireless communication networks. *IEEE Commun. Mag.* **2014**, *52*, 122–130.
27. Ge, X.; Cheng, H.; Mao, G.; Yang, Y.; Tu, S. Vehicular communications for 5G cooperative small-cell networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 7882–7894.
28. Ge, X.; Li, Z.; Li, S. 5G software defined vehicular networks. *IEEE Commun. Mag.* **2017**, *55*, 87–93.
29. Kiayias, A.; Konstantinou, I.; Russell, A.; David, B.; Oliynykov, R. A Provably Secure Proof-of-Stake Blockchain Protocol. *IACR Cryptol. EPrint Arch.* **2016**, *2016*, 889.
30. Pang, L.; Kou, M.; Wei, M.; Li, H. Efficient Anonymous Certificateless Multi-Receiver Signcryption Scheme Without Bilinear Pairings. *IEEE Access* **2018**, *6*, 78123–78135.
31. Zheng, Y.; Li, M.; Lou, W.; Hou, Y.T. Location based handshake and private proximity test with location tags. *IEEE Trans. Dependable Secur. Comput.* **2017**, *14*, 406–419.
32. Kiayias, A.; Russell, A.; David, B.; Oliynykov, R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference*; Springer: Cham, Switzerland, 2017; pp. 357–388.
33. Selvi, S.S.D.; Vivek, S.S.; Shukla, D.; Chandrasekaran, P.R. Efficient and provably secure certificateless multi-receiver signcryption. In *International Conference on Provable Security;* Springer: Berlin/Heidelberg, Germany, 2008; pp. 52–67.
34. Wei, D. Crypto++ Library 5.6.5, a Free C++ Class Library of Cryptographic Schemes. 2019. Available online: http://www.cryptopp.com (accessed on 29 August 2019).
35. He, D.; Zeadally, S.; Xu, B.; Huang, X. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691.
36. BBCNews. 5G Researchers Manage Record Connection Speed, 2015. 2019. Available online: http://www.bbc.co.uk/news/technology-31622297 (accessed on 29 August 2019).