sensors

MDPI

Article

Secure and Lightweight Cloud-Assisted Video Reporting Protocol over 5G-Enabled Vehicular Networks

Lewis Nkenyereye, Joonho Kwon and Yoon-Ho Choi *

School of Computer Science and Engineering, Pusan National University, Busan 46241, Korea; nkenyele@pusan.ac.kr (L.N.); jhkwon@pusan.ac.kr (J.K.)

* Correspondence: yhchoi@pusan.ac.kr; Tel.: +82-51-510-2871

Received: 7 August 2017; Accepted: 18 September 2017; Published: 23 September 2017

Abstract: In the vehicular networks, the real-time video reporting service is used to send the recorded videos in the vehicle to the cloud. However, when facilitating the real-time video reporting service in the vehicular networks, the usage of the fourth generation (4G) long term evolution (LTE) was proved to suffer from latency while the IEEE 802.11p standard does not offer sufficient scalability for a such congested environment. To overcome those drawbacks, the fifth-generation (5G)-enabled vehicular network is considered as a promising technology for empowering the real-time video reporting service. In this paper, we note that security and privacy related issues should also be carefully addressed to boost the early adoption of 5G-enabled vehicular networks. There exist a few research works for secure video reporting service in 5G-enabled vehicular networks. However, their usage is limited because of public key certificates and expensive pairing operations. Thus, we propose a secure and lightweight protocol for cloud-assisted video reporting service in 5G-enabled vehicular networks. Compared to the conventional public key certificates, the proposed protocol achieves entities' authorization through anonymous credential. Also, by using lightweight security primitives instead of expensive bilinear pairing operations, the proposed protocol minimizes the computational overhead. From the evaluation results, we show that the proposed protocol takes the smaller computation and communication time for the cryptographic primitives than that of the well-known Eiza-Ni-Shi protocol.

Keywords: 5G cellular network; cloud assisted vehicular networks; security; video reporting

1. Introduction

Due to the merits of the fifth-generation (5G) cellular networks such as higher mobility support, massive connectivity and reduced latency [1], the academia and industry have shown interest in the 5G technology as a shifting paradigm which overcomes the limitations of the fourth generation (4G) technology. For example, leading companies in IT such as Cisco has predicted that the 5G cellular networks could meet the global mobile data traffic projections for the next five years [2]. That is, it is expected that the 5G cellular networks through the *massive connectivity* property will enable the connection of millions of devices including vehicles.

Especially, 5G cellular networks were embraced as the ultimate framework which would help the implementation of vehicular related technologies [3–5]. For example, a driverless vehicle was tested over 5G cellular networks by *Uber* in the beginning of the year 2017 [6]. Let us note that vehicular network is still in its architectural stage regardless of considerable amount of research works available in the literature [7–10]. Also, security and privacy threats, lack of scalability and latency due to the high mobility of the vehicles are considered as the main reasons that delay the real deployment of vehicular networks. In practice, the researchers have proved that even IEEE 802.11p lacks of mobility support [7] and the Long Term Evolution (LTE) network does not support the effective latency for the vehicular networks [11–13]. Thus, the predicted performance of 5G cellular network in terms of latency, mobility and so on has been considered as a promising archetype for the practical implementation of the intelligent transportation system (ITS)-related services through the cloud assisted vehicular network.

Before the full deployment of the 5G cellular network in the year 2020 [14], security and privacy related issues should be carefully addressed to boost its adoption [15,16]. Furthermore, the ITS services based on the innovative 5G cellular network will require strong security because the data packets are relayed in the safety-critical vehicular environment [17]. That is, the design of secure protocols for the 5G-enabled ITS-related services is required.

To send the videos recorded by the vehicle's cameras into the cloud server, we propose a secure and lightweight cloud-assisted video reporting protocol for 5G-enabled vehicular networks. Recently, Eiza et al. [18] and Yoo [19] have proposed the secure cloud-assisted video reporting protocols in the 5G-enabled networks. By including handover and certificate revocation algorithms, Yoo enhanced the Eiza-Ni-Shi protocol that was designed by using public key certificates. In this paper, we focus on resolving the following drawbacks of the Eiza-Ni-Shi protocol:

- The Eiza-Ni-Shi protocol relies on convectional public key certificates that should be renewed in the vehicle periodically, e.g., every year. However, such periodic renewal is proved to be burdensome over the vehicular networks [20–22].
- The Eiza-Ni-Shi protocol is built on expensive pairing operations. Thus, the overall efficiency of the Eiza-Ni-Shi protocol can be decreased despite the merits of 5G cellular networks.
- The Eiza-Ni-Shi protocol is designed by using an attribute-based encryption. When attribute-based encryption is used to achieve access control, the video sender should know the public key of the receiver. This preliminary makes the Eiza-Ni-Shi protocol to be only applicable in limited services.

Also, we note that the cloud-assisted video reporting protocol should be designed to fulfill security requirements such as privacy, authorization and fine-grained access control over the vehicles. For example, the sender's personal data should not be revealed to unauthorized entities or even the reporting vehicles should not be traced by any malicious users. Even under the huge computation capabilities of 5G-enabled vehicular network, the cloud entities should not waste much time and computation capabilities before they discard bogus, unauthenticated and unauthorized videos. In addition, for the proposed protocol to attain the *non-repudiation* property, the conditional traceability of all the vehicles should be achieved.

To fulfill the above-mentioned goals of 5G-enabled cloud-assisted video reporting protocol and to overcome the drawbacks of the Eiza-Ni-Shi protocol, we propose a new secure and lightweight video reporting protocol for 5G-enabled vehicular networks. We summarize the contributions of this work as follows:

- We define an application model for a secure and lightweight cloud-assisted video reporting protocol over 5G-Enabled vehicular networks. The model highlights the security objectives that the protocol should satisfy within the 5G-Enabled vehicular networks architecture.
- We develop a secure and lightweight cloud-assisted video reporting protocol for 5G-enabled vehicular networks. Without using the conventional public key certificates, the proposed protocol supports entities' *authorization* through anonymous credential. Since the reported videos are broadcasted by the fixed entities, the designated vehicles can recover the reported videos without making any time-consuming communication. Also, by using lightweight security primitives, the proposed protocol minimizes the computation overhead and meets the performance requirement for the real-time ITS-based services in 5G-Enabled vehicular networks.
- We evaluate the performance of the proposed protocol in terms of security objectives, computation cost and communication overhead.

The rest of this paper consists of as follows. After we describe the related work in Section 2, cryptographic primitives for constructing the proposed protocol are overviewed in Section 3.

After describing the overall operation of the proposed protocol in Section 4, we show the detailed operations in Section 5. In Section 6, we show the performance analysis results of the proposed protocol. Finally, we conclude this paper in Section 7.

2. Related Work

In this section, we overview the evolution of vehicle communication architectures for supporting the video reporting service in 5G-enabled vehicular networks.

2.1. VANETs and 5G-Enabled Cloud-Assisted VANETs

As an extension of mobile ad-hoc networks (MANETs) [23], the main entities in vehicular ad hoc networks (VANETs) include the vehicles, the fixed infrastructures along the roads, called road side units (RSU), and an over-viewer third party, called Trusted Authority (TA), in charge of registration, certification and revocation of all the entities within the VANETs architecture. Commonly, VANETs architecture is classified into two main communication means namely vehicle-to-vehicle (V2V) and vehicle to infrastructure (V2I) [24]. The computational cost for the value-added applications in VANETs requires huge computation capabilities, which led to the mixture of VANETs and cloud computing, called *VANETs using Cloud* [25]. *VANETs using Cloud* is defined as vehicular networks equipped with smart devices which communicate with the cloud in the same way as our mobile phones connect to different servers located in the cloud. *VANETs using Cloud* was introduced in [26] by Olariu et al. for the first time. Olariu et al. suggested an autonomous vehicular cloud (AVC) architecture as a special case of *VANETs using Cloud*. In [27], Hussain et al. presented additional services by combining cloud computing and VANETs: Computing as a Service (CompaaS), Storage as a Service (STaaS), Network as a Service (NaaS), Cooperation as a Serivce (CaaS), Entertainment as a Service (ENaaS), Information as a Service (INaaS) and Traffic-Information as a Service (TIaaS). Hussain et al. pointed out the feasibility of *VANETs using Cloud* compared to convectional VANETs. Also, the feasibility of *VANETs using Cloud* was approved by several researchers [28–32]. *Vehicular Cloud* refers to the full utilization of vehicle devices as computers to form mobile servers. In this architecture, one could use the vehicle's OBU to make his/her personal cloud. As a combination of *Vehicular cloud* and *VANETs using Cloud*, *Hybrid vehicle cloud* was proposed. The proposed protocol is built on *VANETs using Cloud* framework, i.e., cloud-assisted vehicular networks. In the following sections, vehicular networks and cloud-assisted vehicular networks are used interchangeably.

2.2. Security and Video Reporting in 5G Enabled Vehicular Network

Security and privacy related topics in 5G cellular networks have mostly being dedicated to security threats of each of the distinct technology (SDN or NFV) [33,34]. Among relevant works on security concerns over 5G cellular network, Mantas et al. [35] surveyed probable threats and attacks against the core modules of 5G cellular networks. The authors also confirmed the four conventional attractive targets in the 4G cellular network: user equipment (UE); access network; the mobile operator's core network; and external Internet Protocol networks. Yang et al. [36] suggested that much effort should be paid on the physical layer of the 5G cellular network. The malicious users are likely to take advantage of the deficiencies of the wireless communication medium such as the poor signal reception quality. Some notable solutions proposed by the authors on the physical layer include artificial noise, confidential and antenna correlation. Alam et al. [37] proposed a framework that analyzes the security requirements of the three scenarios of device to device (D2D) communications in LTE Advanced (LTE-A) networks. The first one includes the network-covered D2D communication without user applications, in which all the nodes in the proximity are under an LTE-A network coverage and the user applications do not need D2D communications. The following scenario is the network-covered D2D communication, where all the devices including the users' devices are covered by an LTE-A network. The last scenario is the network-absent D2D communication. For all these three types of

D2D scenarios, conventional security attacks such as eavesdropping, impersonation attack and the corresponding countermeasure solutions were introduced [37].

For vehicular environment, several researches have addressed potential security and privacy issues in VANETs [38–41]. ITS based services such as navigation services received much attention for the last decade [22,42]. Other protocols in the literature addressed multiple services in VANETs [43–45] for the VANETs integrated with cloud computing. However, all the afore-mentioned protocols are not based on HetNet architecture such as 5G-enabled vehicular network, where our protocol is built upon. Recently, researchers in [18,19] introduced secure and privacy aware cloud-assisted video reporting service in 5G-Enabled vehicular network. However, as noted in Section 1, their protocols have some limitations. This, the design of a new secure and lightweight cloud-assisted video reporting protocol over 5G-enabled vehicular networks is required.

3. Preliminary

We overview the preliminary security properties such as attribute-based encryption (ABE) and certificateless signature scheme.

3.1. Attribute-Based Encryption Scheme

The ABE scheme in [46] is designed for elliptic curve cryptography and is made of the following sub-protocols: Setup, Encryption, Key-Generation, and Decryption algorithms.

3.1.1. ABE.Setup

For the universe of attributes $U = \{1, 2, ..., n\}$; let G_1 be an additive group with a prime order q and $P \in G_1$, where G_1 is made of points on an elliptic curve and P is a generator of G_1. ABE.Setup() sub-protocol works as follows:

- On input of a random $s \in Z_q^*$ as the attribute master secret key, output the corresponding public key $PK = s \cdot P$.
- For each $i \in U$, choose an attribute secret $l_i \in Z_q^*$ to generate the attribute public key $P_i = l_i \cdot P$.
- Set $ABEmk = \{s, l_1, ..., l_{|U|}\}$ and $ABE.params = \{PK, P_1, ..., P_{|U|}\}$.
- Returns $\langle ABEmk, ABE.params \rangle$.

3.1.2. ABE.ENC

For a message m, ω as attribute set, and $ABE.params$, ABE.ENC(m, ω, $ABE.params$) returns the ciphertext CM as follows:

- On input of $k \in Z_q^*$, then output the key $K = k \cdot PK$.
- Compute $C = Enc_K(m)$.
- For $i \in \omega$, compute $W_i = k \cdot P_i$, respectively.
- Output the ciphertext $CM = \langle \omega, C, \{W_i \mid i \in \omega\} \rangle$.

3.1.3. ABE.KGN

ABE.KGN($ABEmk$, Γ) algorithm outputs the shared secret for the decryption keys under the attribute set ω, which consists of a master secret $ABEmk$ and the access tree Γ.

- Based on access tree Γ, allocate index to every node other than root.
- A polynomial $q_{node}(x)$ over Z_q^* is set in top-down manner for each node where each polynomial is of degree $d_{node} - 1$ and d_{node} is considered as the threshold value of the node.
  - Set $q_{root}(0) = s$ for the root node.
  - Set $q_{node}(0) = q_{parent}(index(node))$ for every node with a leaf, where $index(node)$ represents the node's index value.

- Suppose Γ contains n leaves, for every leaf node $leaf_f$ $(1 \leq f \leq n)$, a secret share for the decryption key is generated as $D_{leaf_f} = q_{leaf_f}(0) \cdot t_i^{-1}$ where i represents the attribute linked to $leaf_f$ and l_i a random number for i taken in ABE.Setup.
- Output $D = \{D_{leaf_f} \mid leaf_f \in \Gamma\}$.

3.1.4. ABE.DEC

ABE.DEC(CM, D, $ABE.params$) performs the decryption of the cipher text CM, as long as the attributes set ω fulfills the access tree Γ, by using NodeKey(CM, D, $node$) for every node within the access tree recursively. In this ABE scheme [46], secret sharing based on Lagrange interpolation is borrowed to recover the decryption key.

- For every leaf node linked to an attribute i, NodeKey(CM, D, $leaf_f$) is computed as follows. Note that we represent NodeKey(CM, D, $leaf_f$) into N_1 in the next paragraph for convenience.

  1. In case the associated attribute i to $leaf_f$ is not comprised in ω, then NodeKey(CM, D, $leaf_l$) = $\perp$.
  2. else,

$$\begin{aligned} \mathrm{N}_1 &= D_{leaf_f} \cdot W_i \\ &= q_{leaf_f}(0) \cdot t_i^{-1} \cdot k \cdot P_i \\ &= q_{leaf_f}(0) \cdot t_i^{-1} \cdot k \cdot l_i \cdot P \\ &= q_{leaf_f}(0) \cdot k \cdot P \end{aligned}$$

- To proceed with a non-leaf node u, the algorithm calls NodeKey(CM, D, z) for all children z which are attached to the node u.

  1. Suppose that ω_u is an arbitrary d_u set of children nodes satisfying NodeKey(CM, D, z) $\neq \perp$. In case no such set is existent, NodeKey(CM, D, u) output $\perp$. We use N to denote NodeKey(CM, D, u) in the next paragraph for paper formatting.
  2. Else, let $\Delta_{index(z),\omega'_u} = \prod_{j \in \omega'_u, j \neq index(z)} \frac{x-j}{i-j}$ represent the Lagrange coefficient with $\omega'_u = \{index(z) \mid z \in \omega_u\}$,

$$\begin{aligned} \mathrm{N} &= \sum_{z \in \omega_u} \Delta_{index(z),\omega'_u}(0) \cdot \mathrm{NodeKey}(CM, D, z) \\ &= \sum_{z \in \omega_u} \Delta_{index(z),\omega'_u}(0) \cdot q_z(0) \cdot k \cdot P \\ &= \sum_{z \in \omega_u} \Delta_{index(z),\omega'_u}(0) \cdot q_{parent}(index(z)) \cdot k \cdot P \\ &= \sum_{z \in \omega_u} \Delta_{index(z),\omega'_u}(0) \cdot q_u(index(z)) \cdot k \cdot P \\ &= q_u(0) \cdot k \cdot P \end{aligned}$$

- Compute the decryption key K = NodeKey(CM, D, $root$) = $q_{root}(0) \cdot k \cdot P = s \cdot k \cdot P$.
- Output the decrypted message $m = Dec_K(C)$.

3.2. Certificateless Signature Scheme

Certificateless signature scheme (CertS) [47] consists of the following procedures.

- CertS.Setup() computes a master key along with a public system parameters as follows:
  - Let G be an additive group with a prime order q and $P \in G$ be a generator based on an elliptic curve.

  - Choose $s \in Z_q^*$ as master secret key and generates the master public key $P_{pub} = s \cdot P$.
  - Let $H_1 : \{0,1\}^* \times G \rightarrow Z_q^*$ and $H_2 : \{0,1\}^* \times G \rightarrow Z_q^*$ be two cryptographic hash functions.
  - Output the public parameters $CertS.params = \{G, q, P, P_{pub}, H_1, H_2\}$.
  - Output $\langle s, CertS.params \rangle$

- CertS.Secret(id) returns a secret value for every identity id as follows:

  - Choose $x_{id} \in Z_q^*$ as a secret value, then compute $P_{id} = x_{id} \cdot P$.
  - Return $Sec_1 = \langle x_{id}, P_{id} \rangle$

- CertS.PartialK(s, id, P_{id}) computes a partial private/public key for the given id as follows:

  - Select a random $r_{id} \in Z_q^*$ and generate $R_{id} = r_{id} \cdot P$.
  - Compute $s_{id} = r_{id} + s \cdot H_1(id, R_{id}, P_{id})$ (mod q).
  - Output $Sec_2 = \langle s_{id}, R_{id} \rangle$ as the corresponding partial private key.

- CertS.SKey(Sec_1, Sec_2) sets $sk_{id} = \langle x_{id}, s_{id} \rangle$ and $pk_{id} = \langle P_{id}, R_{id} \rangle$ representing the private key and public key for id, respectively.
- CertS.Sign(m, sk_{id}) computes the signature for a given message m as follows:

  - Select a random $l \in Z_q^*$ such that gcd($l + h$, q) = 1, where $h = H_2(m, R, P_{id}, R_{id})$ and $R = l \cdot P$.
  - Generates $r = (l + h)^{-1}(x_{id} + s_{id})$ (mod q).
  - Output the signature $\sigma = \langle r, R \rangle$.

- CertS.Verify(m, id, pk_{id}, σ) provides the signature verification σ for the message m for the identity id as follows:

  - Generate $h_1 = H_1(id, R_{id}, P_{id})$ and $h_2 = H_2(m, R, id, P_{id}, R_{id})$.
  - Check whether $r \cdot (R + h_2 \cdot P) \overset{?}{=} P_{id} + R_{id} + (h_1 \ \cdot P_{pub})$.

4. Overview of Proposed Protocol

After overviewing the system architecture and describing the security requirements, we explain the overall operation of the proposed protocol.

4.1. System Architecture

As a major difference from the convectional cloud assisted vehicular network architecture, the 5G-Enabled vehicular network is deployed on the following communication mediums:

- Heterogeneous Networks: This network is originated from the ultimate desire to achieve high data rate and network capacity for the 5G-enabled network. Thus, two solutions may help to attain the aforementioned capacities by making the size of cells smaller and embracing the mmWave spectrum. Making the size of the cell much smaller would increase the spectral efficiency [48]. On the other side, the mmWave communications will offer high data rates because it operates in the range of 30–300 GHz and 1–10 mm for the spectrum and wavelength respectively. As mentioned in [38], the mmWave technology still suffers from considerable propagation loss that generates tremendous line of sight (LOS) connections.
- D2D Communications: D2D communication enables devices to communicate with each other within the licensed cellular bandwidth without involving the BS. In the 5G-Enabled vehicular networks, the vehicles can communicate through D2D communication or by direct link under the mmWare technology.

We describe the communication entities in the proposed protocol: TA, DV, DMV, RSC and vehicles that communicate through the on board unit (OBU) as shown in Figure 1.

- Trusted Authority (TA): It is in charge of the registration of all entities (DMV, DV, RSC and vehicles) inside our system and issues cryptographic materials during the system initialization.
- Department of Motor Vehicles (DMV): All the vehicles are assumed to register with the DMV periodically. Beside the conventional techniques for vehicle's identification including the Electronic License Plate (ELP) or the Electronic Chassis Number (ECN), each vehicle is registered with a 5G identifier (5GID) with the same functionalities as the subscriber identification module (SIM) chip.
- Road Side cloud (RSC): RSCs are servers located along the roads and accessible by the vehicles. RSCs stores the videos files (VFs) sent by the vehicles. In that case, the designated vehicles (DV) such as police or ambulance can download the files through the RSCs using mmWare communications. Due to the advancements of technology, we assume that RSCs are connected to an electricity power generator with enough computational capability.
- Designated Vehicles: The designated vehicles can be public or private vehicles registered by the government through the DMV that offers public services.
- Vehicles: Vehicles are equipped with OBUs which allow them to communicate with RSCs in order to send the recorded video files.

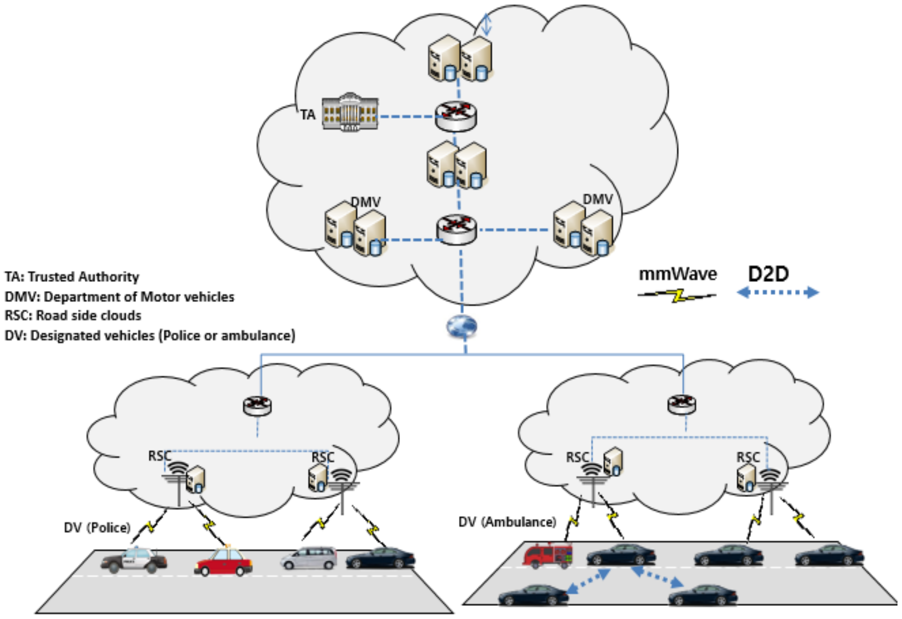

Figure 1. System Architecture.

4.2. Security Objectives

The proposed protocol is designed to satisfy the following security requirements.

- Authentication and Authorization: Any vehicle has to be authenticated before it can send (report) a video recorded by its camera.
- Identity privacy preservation: The real identity of every vehicle should be protected from being known by other vehicles, RSC, DVs and DMV.
- Fine-grained access control: ABE should guarantee a fine-grained access control by which a designated vehicle should strictly be capable to recover a video fitting to its possessed access structure.
- Non-repudiation: A given vehicle should not deny its participation in video reporting.
- Traceability: TA should be capable of disclosing the real identity of all the entities in the system.

4.3. Overall Operation

The overall operation of the proposed protocol consists of system setup, periodic credential generation, on-duty token generation and accident Reporting procedures.

- System setup: 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 from which a partial private key is computed. DMVs and RSCs also provide their real identities and TA computes their partial private keys. Each vehicle registers with the TA through the DMV, the designated vehicles such as the police or ambulance also register with the TA through the DMV.
- Periodic credential generation: Periodically, a vehicle request for credential in order report the recorded videos. DMV generates the periodic credential to vehicles along with the set of attributes corresponding to the type of request. We assume that based on some criteria such as accident record or reckless driving, DMV can decide to give different set of attributes to participating vehicles.
- On-duty token generation: The designated vehicles also received on-duty tokens. These tokens will be used by the designated to retrieve reported videos from the RSCs.
- Accident Reporting: Periodically, a vehicle registers for road reporting services. During the registration, the vehicle specifies the types of services to be reported such as accident or abnormal scene (we assume that the camera of a vehicle is not limited to report road's accidents only). An incentive technique based on point accumulation could be considered in order to motivate the vehicle users to participate in video reporting. Whenever an accident or abnormal scene occurs the camera records the scene and upload the files to the RSC using mmWare technology or D2D communication. The designated vehicles would later on acquire the report from the RSCs as long as they possess enough access structure to recover the secret.

5. Details of Proposed Protocol

In this section, we describe the secure and lightweight cloud assisted video reporting protocol over 5G-enabled vehicular networks in details. In Table 1, we summarize the notations used for the proposed protocol and the overall operations of the protocol are depicted in Figure 2.

Table 1. Terminology.

Term	Notation
$5G_{ID}$	Unique 5G identity for each OBU's vehicle
TA	Trusted Authority
DMV_k	Department of Motor vehicle's server
RSC_j	Roadside cloud's server
DV_j	Identity of designated vehicle's OBU
R-cred	v_i's credential issued by DMV_k
KN	Key word within a vehicle's credential
$List_{KN}$	List of generated KNs periodically
Tok_{DV}	A duty token for DV_j generated by DMV_j
$alias_i$	v_i's pseudo identity
ts	time stamp
δ_i	certificateless signature of entity i
$\mathbb{G}$	Elliptic curve group with the same order q
$P \in \mathbb{G}_1$	A generator of $\mathbb{G}_1$
sk_{id}, pk_{id}	private, public key pair of an entity X
t_i	Master secret for each attribute i
$ABE.amk$	Attribute master key
T_i	Public key for each attribute $i \in U$
$alias_{v_i}$	v_i's pseudonym
U	Universe of attribute
Γ	Access tree
ω	Attribute set
AS_j	Access Structure corresponding to entity j
D	Set of secret share D_{leaf_l} in Γ
$Enc_k(.)$	Symmetric encryption under key k

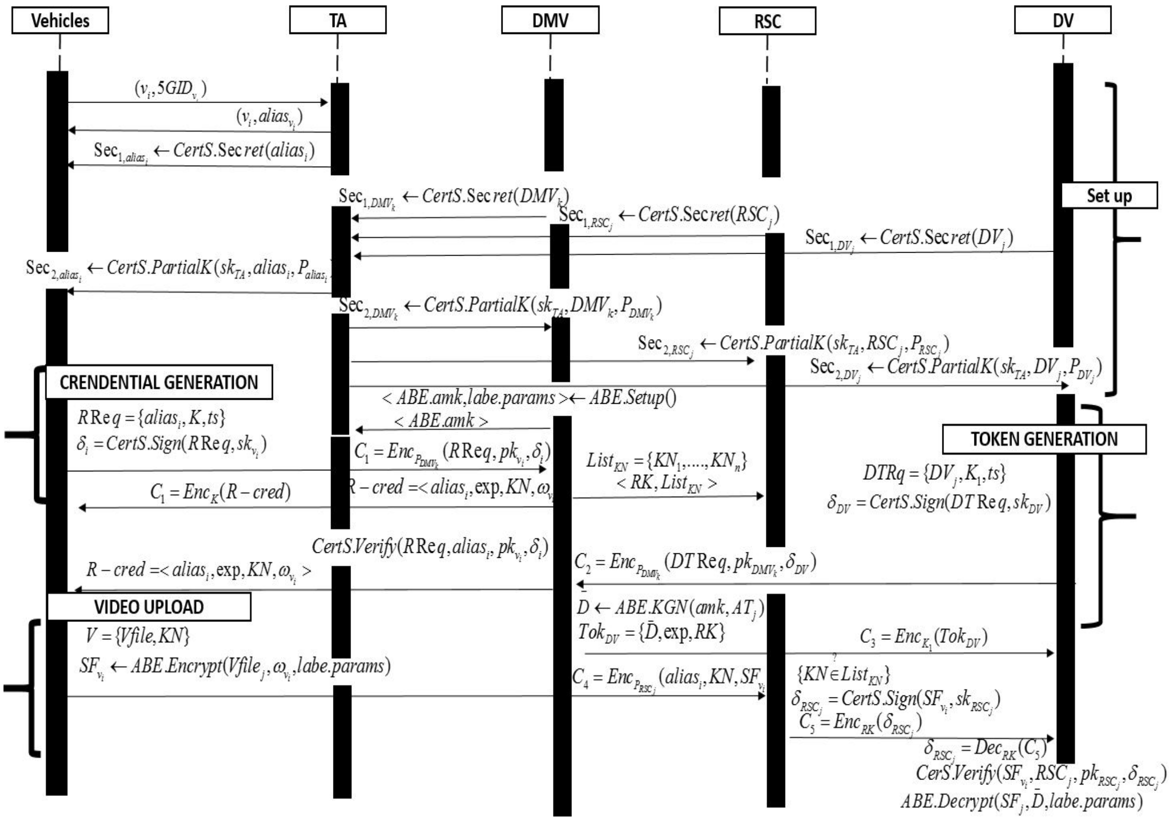
Vehicles
TA
DMV
RSC
DV
$(v_i, 5GID_{v_i})$
$(v_i, alias_{v_i})$
$\mathrm{Sec}_{1,alias_i} \leftarrow CertS.\mathrm{Sec}ret(alias_i)$
Set up
$\mathrm{Sec}_{1,DMV_k} \leftarrow CertS.\mathrm{Sec}ret(DMV_k)$
$\mathrm{Sec}_{1,RSC_j} \leftarrow CertS.\mathrm{Sec}ret(RSC_j)$
$\mathrm{Sec}_{1,DV_j} \leftarrow CertS.\mathrm{Sec}ret(DV_j)$
$\mathrm{Sec}_{2,alias_i} \leftarrow CertS.PartialK(sk_{TA}, alias_i, P_{alias_i}$
$\mathrm{Sec}_{2,DMV_k} \leftarrow CertS.PartialK(sk_{TA}, DMV_k, P_{DMV_k})$
$\mathrm{Sec}_{2,RSC_j} \leftarrow CertS.PartialK(sk_{TA}, RSC_j, P_{RSC_j})$
$\mathrm{Sec}_{2,DV_j} \leftarrow CertS.PartialK(sk_{TA}, DV_j, P_{DV_j})$
CRENDENTIAL GENERATION
$< ABE.amk, labe.params > \leftarrow ABE.Setup()$
$< ABE.amk >$
$R\mathrm{Re}q = \{alias_i, K, ts\}$
$\delta_i = CertS.Sign(R\mathrm{Re}q, sk_{v_i})$
$C_1 = Enc_{P_{DMV_k}}(R\mathrm{Re}q, pk_{v_i}, \delta_i)$
$R - cred =< alias_i, \exp, KN, \omega_{v_i}$
$C_1 = Enc_K(R - cred)$
$List_{KN} = \{KN_1, ..., KN_n\}$
$< RK, List_{KN} >$
TOKEN GENERATION
$DTRq = \{DV_j, K_1, ts\}$
$\delta_{DV} = CertS.Sign(DT\mathrm{Re}q, sk_{DV})$
$CertS.Verify(R\mathrm{Re}q, alias_i, pk_{v_i}, \delta_i)$
$R - cred =< alias_i, \exp, KN, \omega_{v_i} >$
$C_2 = Enc_{P_{DMV_k}}(DT\mathrm{Re}q, pk_{DMV_k}, \delta_{DV})$
VIDEO UPLOAD
$\bar{D} \leftarrow ABE.KGN(amk, AT_j)$
$Tok_{DV} = \{\bar{D}, \exp, RK\}$
$V = \{Vfile, KN\}$
$SF_{v_i} \leftarrow ABE.Encrypt(Vfile_j, \omega_{v_i}, labe.params)$
$C_3 = Enc_{K_1}(Tok_{DV})$
$C_4 = Enc_{P_{RSC_j}}(alias_i, KN, SF_{v_i}$
$\{KN \overset{?}{\in} List_{KN}\}$
$\delta_{RSC_j} = CertS.Sign(SF_{v_i}, sk_{RSC_j})$
$C_5 = Enc_{RK}(\delta_{RSC_j})$
$\delta_{RSC_j} = Dec_{RK}(C_5)$
$CerS.Verify(SF_{v_i}, RSC_j, pk_{RSC_j}, \delta_{RSC_j})$
$ABE.Decrypt(SF_j, \bar{D}, labe.params)$

Figure 2. Protocol description.

5.1. System Setup

In setup phase, TA generates global system parameters and all the entities register to the TA as follows:

1. TA selects an elliptic curve group $\mathbb{G}_1$ of order q with $P \in \mathbb{G}_1$ as a generator.
2. In order to get the master secret sk_{TA} and public key pk_{TA}, TA executes CertS.Setup() and sets $\langle sk_{TA}, CertS.params \rangle \leftarrow$ CLS.Setup(), then output $CertS.params$.
3. In order to keep a record of each vehicle v_i, TA set a pseudonym $alias_{v_i}$ to every v_i based on its real identity $5GID_{v_i}$.
4. Each RSC_j, DV_j and DMV_k registers to TA, then computes CertS private keys as follows:
   - RSC_j, DV_j and DMV_k computes $Sec_{1,RSC_j} \leftarrow$ CertS.Secret(RSC_j), $Sec_{1,DV_j} \leftarrow$ CertS.Secret(DV_j)
     and $Sec_{1,DMV_k} \leftarrow$ CertS.Secret(DMV_k), and makes a request for partial private key to the TA, respectively.
   - TA provides $Sec_{2,RSC_j} \leftarrow$ CertS.PartialK(sk_{TA}, RSC_j, P_{RSC_j}); $Sec_{2,DV_j} \leftarrow$ CertS.PartialK(sk_{TA}, DV_j, P_{DV_j}) and
     $Sec_{2,DMV_k} \leftarrow$ CertS.PartiaK(sk_{TA}, DMV_k, P_{DMV_k}) to each entity securely.
   - RSC_j, DV_j and DMV_k set $\left\langle sk_{RSC_j}, pk_{RSC_j} \right\rangle \leftarrow$ CertS.SKey(Sec_{1,RSC_j}, Sec_{2,RSC_j}); $\left\langle sk_{DV_j}, pk_{DV_j} \right\rangle \leftarrow$ CertS.SKey(Sec_{1,DV_j}, Sec_{2,DV_j}) and $\langle sk_{DMV_k}, pk_{DMV_k} \rangle \leftarrow$ CertS.SKey(Sec_{1,DMV_k}, Sec_{2,DMV_k}), respectively.
5. Likewise, every v_i computes $Sec_{1,v_i} \leftarrow$ CertS.Secret($alias_i$), TA provides $Sec_{2,v_i} \leftarrow$ CertS.PartialK(sk_{TA}, $alias_i$, P_{v_i}), then v_i sets
   $\langle sk_{v_i}, pk_{v_i} \rangle \leftarrow$ CertS.SKey(Sec_{1,v_i}, Sec_{2,v_i}).

6. DMV_k selects a given universe of attributes $U = \{1, ..., N\}$, computes ABE parameters as $\langle ABE.amk, labe.params \rangle \leftarrow$ ABE.Setup(), then avails $labe.params$ to the whole system. Note that $DMVs$ will later send $ABE.amk$ to TA in non busy hours.

5.2. Periodic Credential Generation

Periodically (on a daily basis), the vehicles request a road reporting credential ($RReq$) which permits the reporting of the abnormal scenes captured by the vehicle's camera. To acquire a RReq from DMV_k, v_i performs the following:

- v_i composes a credential request message $RReq = \{alias_i, K, ts\}$ where ts is the time stamp and K is a secret key to be used later.
- v_i sends $C_1 = Enc_{PK_{DMV_k}}\{RReq, pk_{v_i}, \delta_i\}$ to the DMV_k, where δ is the signature for the $RReq$ set as δ_i = CertS.Sign($RReq$, sk_{v_i}).
- Upon receiving the message C_1, DMV_k first decrypts C_1 using its private key, then verifies the signature as CertS.Verify($RReq$, $alias_i$, pk_{v_i}, δ).

If it holds, DMV_k generates reporting credential (R-$cred$) as follows:

1. Generate $R\text{-}cred = \langle alias_i, exp, KN, \omega_{v_i} \rangle$ where exp is the expiration date, ω_{v_i} the set of attributes and KN the keyword for the credential. Note that KN is not specific for each credential but is the same based on the access structure.
2. DMV_k sends $C_1 = Enc_K(R\text{-}cred)$ to v_i. Then, v_i can recover R-$cred$ by decrypting the C_1 under the shared secret key K.
3. DMV_k sends periodically a list $List_{KN}$ of all the keywords enclosed in the credentials to $RSCs$.

5.3. On-Duty Token Generation

In the same way, DMV_j generates on-duty token for the designated vehicles. These tokens authorize the DVs to recover the reported videos. For instance a police vehicle can get an *on-duty token* which extends its duty from police's duties to basic ambulance's duties. If an area A witnesses numerous accidents, several ambulances would go to the accident's scenes in area A which might cause a temporal non-availability of ambulances. In that case, some of the police agents which have basic medical skills can attend to accident's victims as they wait for the ambulances to arrive.

1. DV_i composes an on-duty token request $DTRq = \{DV_j, K_1, ts\}$ where ts is the time stamp and K_1 is a secret key to be used later.
2. DV_i sends $C_2 = Enc_{PK_{DMV_k}}\{DTReq, pk_{v_i}, \delta_{DV}\}$ to the DMV_k, where δ_{DV} is the signature for the $DTRq$ set as δ_{DV} = CertS.Sign($DTRq$, sk_{DV}).
3. Upon receiving the message C_2, DMV_k first decrypts C_2 using its private key, then verifies the signature as CertS.Verify($DTRq$, DV_j, pk_{DV_j}, δ_{DV}).
4. DMV_j set $\bar{D} \leftarrow$ ABE.KGN($ABE.amk$, AS_{DV_j}) where AS_{DV_j} is the access structure corresponding to the designated vehicle's type (police or ambulance).
5. DMV_j composes a token message $Tok_{DV} = \{\bar{D}, exp, RK\}$ where exp is the expiring date, RK a shared secret which is given to DVs that are supposed to work within a defined geographic zone. Note that in real word, one police vehicle can be assign to attend to all the requests from a defined geographic area (three or five consecutive streets). DMV_j send it to DV_j encrypted under the shared symmetric key K_1 as $C_3 = Enc_{K_1}(Tok_{DV})$.

5.4. Abnormal Video Recording

We assume that the in-built camera has the functionalities which can allow the driver to upload a given file or the camera's sensors can decide to upload a particular video after analyzing abnormal movements within the video [49]. The timing and circumstances techniques in which the video should be uploaded are not within the scope of this paper. The vehicles perform the following before uploading the video file captured by the camera:

1. After recording a video file, v_i composes a message $V = \{Vfile_j, KN\}$; uses the access policy ω_{v_i} retrieved in the credential *R-cred* and encrypts the file under the given attribute set ω_{v_i} as $SF_j \leftarrow$ ABE.Encrypt($Vfile_j$, ω_j, $labe.params$).
2. v_i sends $C_4 = Enc_{PK_{RSC_j}}\{alias_i, KN, SF_j\}$ to RSC_j.
3. RSC_j decrypts C_4 and check if $\{KN \in List_{KN}\}$.
4. If not C_4 is discarded. Note that KN value are similar for all the vehicles which have a similar set of attribute such as ω. As mentioned before, DMV_j can choose to give a type of attributes to a vehicle based on different criteria such accident record and reckless driving record. The choice of those criteria is beyond the scope of this paper.
5. Otherwise, RSC_j forwards the file securely to neighboring $RSCs$.
6. RSC_j generates $C_5^{'} = \delta_{RSC_j}$ = CertS.Sign(SF_j, sk_{RSC_j}) and broadcast $C_5 = Enc_{RK}(C_5^{'})$ within its coverage area.

   After receiving the beacons, DVs performs the following:

- DV_j decrypts $C_5 = Enc_{RK}(C_5^{'})$ using the area shared key of RK. Note that only DVs assigned to work within RSC_j coverage can decrypt the C_5.
- DV_j runs CertS.Verify(SF_j, RSC_j, pk_{RSC_j}, δ_{RSC_j}).
- DV_j runs ABE.Decrypt(SF_j, $\bar{D}$, $labe.params$) to get the original file of $Vfile_j$.

6. Performance Evaluation

In this section, we show the performance evaluation results of the proposed protocol based on security analysis, computational delay and communication overhead.

6.1. Security

The security achievements of the proposed protocol are as follows:

- *Authentication*: The authentication for every v_i requesting a service file is provided by the certificateless signature scheme on message
  $RReq = \{alias_i, K, ts\}$ with $C_1 = Enc_{PK_{DMV_k}}\{RReq, pk_{v_i}, \delta_i\}$. No malicious user can falsify a valid signature based on the hardness of DL problem. Otherwise the verifier could check the validity of the message by running CLS.Verify(m, id, pk_{id}, σ) to check if $r \cdot (R + h_2 \cdot P) \overset{?}{=} P_{id} + R_{id} + (h_1 \ \cdot P_{pub})$. Thus, the authentication is guaranteed for the proposed protocol.
- *Authorization*: Every vehicle has to get a periodic credential before it can participate in video reporting. v_i sends $C_1 = Enc_{PK_{DMV_k}}\{RReq, pk_{v_i}, \delta_i\}$ to the DMV_k to request a credential. After a valid verification, DMV_k sends $C_1 = Enc_K(R - cred)$ where $R - cred = \langle alias_i, exp, KN, \omega_{v_i}\rangle$ as v_i's credential which allows the v_i to participate in video reporting.
- *Identity privacy preservation*: It is hard for an attacker to get a real identity of a vehicle within our proposed protocol. In the registration stage of the vehicle provided by TA, every vehicle v_i is provided with a pseudo-identity $alias_{v_i}$. Though the malicious user would get the credential request message $RReq = \{alias_i, K, ts\}$, the single plain identity of v_i which is available is its pseudo-identity $alias_{v_i}$. In the rest of the protocol, the remaining available information concerning v_i is its pseudo-identity $alias_{v_i}$. We confirm that our protocol achieves identity privacy preservation.
- Fine-grained access control: In the proposed protocol, the video file $Vfile$ sent to v_i is encrypted under a set of attributes as $SF_j \leftarrow$ ABE.Encrypt($Vfile_j$, ω_j, $labe.params$). The file is sent encrypted under the public key of RSC_j.RSC_j only checks if $KN \in List_{KN}$; this will save the $RSCs$ from availing bogus files to DVs. RSC_j can not recover the file. Even for DVs, unless a DV_j possesses

the required secret shares $D_{leaf_l} = q_{leaf_l}(0) \cdot t_i^{-1}$, it cannot reconstruct the root node R to be able to get the secret $q_{root}(0) \cdot k \cdot P = s \cdot k \cdot P$. Throughout the decryption stage based on the root or child node, except DV_j has the obligatory secret shares, the decryption procedure returns $\perp$. Consequently, even the entities (vehicles)that share a certain number of attributes can not conspire (collude) together to recuperate the secret that will achieves the decryption of the video file.

- Non-repudiation: A vehicle can not deny of participating in video reporting because the receiving RSC_j keeps v_i's pseudo identity and its anonymous keyword KN contained in the credential $R - cred = \langle alias_i, exp, KN, \omega_{v_i} \rangle$.
- Traceability: Even though it is hard for an attacker to know the real identity of a vehicle, TA has the capability of revealing the vehicle's real identity in case of disputes. TA makes a search to find which real identity corresponds to any given or reported $alias_{v_i}$. We conclude that the proposed protocol satisfies the traceability property.

6.2. Cost Comparison

We show the analysis results of the computational and communication costs of the proposed protocol.

6.2.1. Computation Cost

When analyzing the computation cost of the proposed protocol, we deliberately omit the time complexity measurement of the setup phase since it is considered to be done offline and infrequently. We basically privilege the operations that dominate the speed of signature generation and verification. We adopt the implementation parameters in [50,51] with embedding degree 6, $\{\mathbb{G}, q\}$ represented by 161 bits and 160 bits respectively. The implementation was performed on a 3.5-GHz, core i-5, 16 GB RAM desktop computer with $crypto++$ library 5.6.5 [52]. The cost of respective security primitives are depicted in Table 2.

Table 2. Measurement of cryptographic operations.

Notation	**Operations**	**Time (ms)**
T_{pair}	Bilinear pairing	4.5
T_{mul}	Point scalar multiplication	0.6
$T_{as\text{-}enc}$	Asymmetric encryption	1.17
$T_{as\text{-}dec}$	Asymmetric decryption	0.61
$T_{s\text{-}enc}$	Symmetric encryption	0.51
$T_{s\text{-}dec}$	Symmetric decryption	0.55
T_h	hash function	0.0001

6.2.2. Overall Cost Including Communication Cost

Note that TA uses secure symmetric encryption/decryption algorithm. For fairness in comparison, we adopt AES/CBC (256-bit key) with a processing speed of 65 MB/s. We also consider the size of the video ranging from 2 to 8 Gigabytes. We use SHA-512 hash function with a processing speed of 231 MB/s. The connection speed for the 5G-enabled vehicular network is set to 1.2 Gb/s and vehicle's velocity to 100 km/h [53]. We also use CP-ABE toolkit [54] along with MIRACL [55] library to benchmark the performance of attribute-based encryption. We set the attribution number to 4 by following the reference [18]. The overall operation involved for signing and verifying is illustrated in Table 3. As being described in Section 5.4, v_i computes $W_i = k \cdot P_i$ and $q_{leaf_l}(0) \cdot t_i^{-1}$; which equals to $(d+1)T_{mul}$ where d is the number of attributes based on the access structure. Furthermore, v_i sends the file encrypted under the public of RSC_j which equals to $T_{as\text{-}enc}$. RSC_j only decrypts the file and check the validity of the KN which was earlier provided within the vehicle credential. In Figure 3, we show the time overhead for encrypting and signing the files recorded by the vehicles' OBUs.

To recover the video file, DV_i decrypts the file in $T_{as\text{-}dec}$ and checks if $r \cdot (R + h_2 \cdot P) \overset{?}{=} P_{id} + R_{id} + (h_1 \ \cdot P_{pub})$ for signature verification in $2T_{mul}$. DV_j computes $q_{leaf_l}(0) \cdot k \cdot P$ in dT_{mul}. On the other hand, the protocol in [18] requires $T_{pair} + T_{mul}$ to perform *public key encryption with key search* [56]; $(d+1)T_{mul} + (d+1)T_{pair}$ for attribute-based encryption and T_{mul} for signature generation. In order to recover the video file, the designated vehicle requires $3T_{pair} + 4T_{mul}$ for certificate and signature verification and $4T_{pair}$ for attribute-based decryption. The total overhead which comprises the required time to encrypt, sign, transmit, verify and decrypt the reported file is shown in Figure 4. It is predicated that the connection speed for the 5G-enabled vehicles will be higher than 1.2 GB/s up to 1 Tb/s which has been already achieved for stationary wireless connection [57]. In Figure 5, we show the overall time overhead with different 5G connection speeds for a 2 GB video file. As shown in Figure 4, the time for the vehicle's OBU to encrypt, sign and decrypt the recorded file in the proposed protocol is also less than the Eiza-Ni-Shi protocol [18] by 50%. These observations show that the proposed protocol offers the possibility to the vehicles that witnessed abnormal events such as road's accidents to report the scene to the designated entities for a timely response.

Table 3. Computational costs of the Eiza-Ni-Shi protocol [18] and the proposed protocol.

Scheme Phase	Eiza et al. [18]	Proposed
Signing/video	$(d+2)T_{mul} + (d+2)T_{pair}$	$(d+1)T_{mul}$
Verification/video	$7T_{pair} + 4T_{mul}$	$(d+3)T_{mul}$
Total cost/ms	64	7.2

(d=number of leaf node).

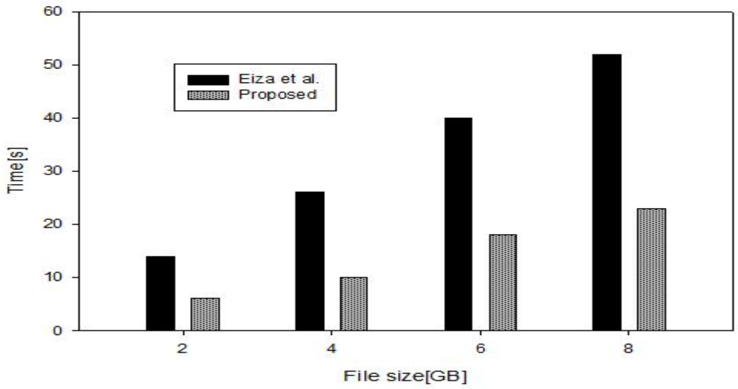

Figure 3. Enccryption/signing cost.

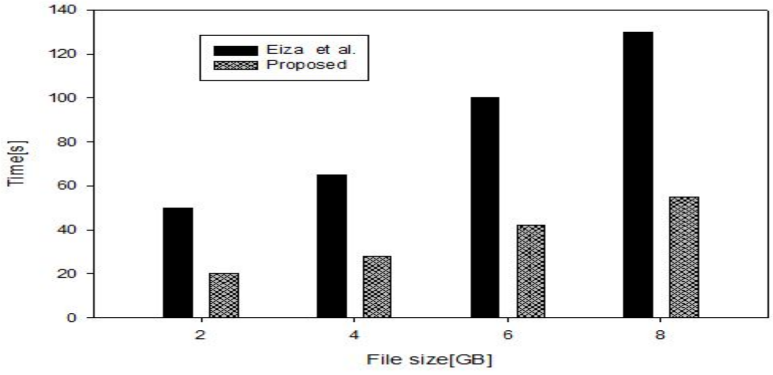

Figure 4. Overall cost.

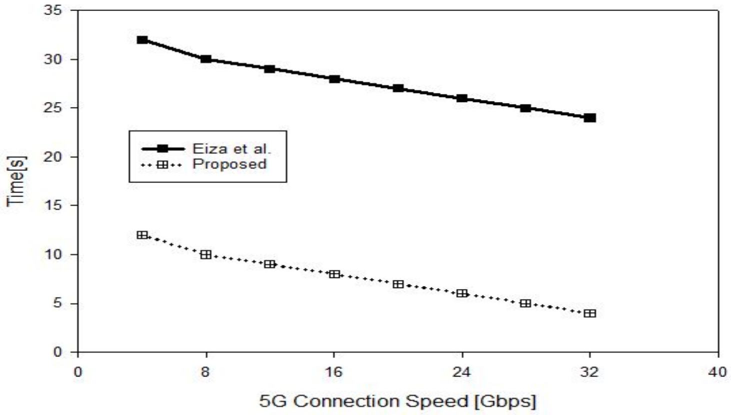

Figure 5. Overall cost under different 5G connection speeds.

7. Conclusions

In this paper, we noted that although there exist a few research works for secure video reporting service in 5G-enabled vehicular networks, their usage is limited because of public key certificates and expensive pairing operations are required. To overcome the limitation, we proposed a new secure and lightweight protocol for cloud-assisted video reporting service in 5G-enabled vehicular networks. Based on a fined-grained access control, the proposed protocol allowed the designated vehicles to recover the recorded video files without any prior communication. By providing security and privacy for the participating entities, the proposed protocol prevents malicious users from tracking, revealing or impersonating the system entities. Also, by using a new certificateless signature scheme, the proposed protocol assured the authentication of legitimate vehicles. With anonymous credentials instead of public key certificates, the proposed protocol guaranteed the authorization of participating entities. From the security and performance analysis results, we showed that the proposed protocol took a lightweight overhead compared to the state-of-the-art works. From these analysis results, we believe that the proposed protocol will help to realize timely and secure cloud-assisted video reporting service over 5G-enabled vehicular networks.

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-2015R1D1A1A01057888), and by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No.2012-0-00265, Development of high performance IoT device and Open Platform with Intelligent Software).

Author Contributions: Lewis Nkenyereye identified the drawbacks in Eiza et al protocol. Then he proposed how the protocol would be improved to overcome the outpointed weaknesses. Yoon-Ho Choi contributed by proposing a new orientation on how the protocol would be enhanced in terms of security primitives. Joon ho Kwon contributed for cryptographic analysis and organizing the sections and subsections of the paper. In this article, all authors have read the final version of the manuscript for approval purpose.

Conflicts of Interest: All the authors confirm that there is no conflict of interest.

References

1. Shen, X. Device-to-device communication in 5G cellular networks. *IEEE Netw.* **2015**, *29*, 2–3.
2. Yu, R.; Ding, J.; Huang, X.; Zhou, M.T.; Gjessing, S.; Zhang, Y. Optimal resource sharing in 5g-enabled vehicular networks: A matrix game approach. *IEEE Trans. Veh. Technol.* **2016**, *65*, 7844–7856.
3. Andrews, J.G.; Buzzi, S.; Choi, W.; Hanly, S.V.; Lozano, A.; Soong, A.C.; Zhang, J.C. What will 5G be? *IEEE J. Sel. Areas Commun.* **2014**, *32*, 1065–1082.
4. Li, Q.C.; Niu, H.; Papathanassiou, A.T.; Wu, G. 5G network capacity: Key elements and technologies. *IEEE Veh. Technol. Mag.* **2014**, *9*, 71–78.

5. Bhushan, N.; Li, J.; Malladi, D.; Gilmore, R.; Brenner, D.; Damnjanovic, A.; Sukhavasi, R.; Patel, C.; Geirhofer, S. Network densification: The dominant theme for wireless evolution into 5G. *IEEE Commun. Mag.* **2014**, *52*, 82–89.
6. Bloom, C.; Tan, J.; Ramjohn, J.; Bauer, L. Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles. In Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS), Santa Clara, CA, USA, 12–14 July 2017; USENIX Association: Berkeley, CA, USA, 2017; pp. 357–375.
7. Bellalta, B.; Belyaev, E.; Jonsson, M.; Vinel, A. Performance evaluation of IEEE 802.11p-enabled vehicular video surveillance system. *IEEE Commun. Lett.* **2014**, *18*, 708–711.
8. 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.
9. 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.
10. Chen, S.; Zhao, J. The requirements, challenges, and technologies for 5G of terrestrial mobile telecommunication. *IEEE Commun. Mag.* **2014**, *52*, 36–43.
11. Belyaev, E.; Vinel, A.; Surak, A.; Gabbouj, M.; Jonsson, M.; Egiazarian, K. Robust vehicle-to-infrastructure video transmission for road surveillance applications. *IEEE Trans. Veh. Technol.* **2015**, *64*, 2991–3003.
12. Eiza, M.H.; Ni, Q.; Owens, T.; Min, G. Investigation of routing reliability of vehicular ad hoc networks. *EURASIP J. Wirel. Commun. Netw.* **2013**, *2013*, 179.
13. Eiza, M.H.; Owens, T.; Ni, Q.; Shi, Q. Situation-aware QoS routing algorithm for vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **2015**, *64*, 5520–5535.
14. Wang, C.X.; Haider, F.; Gao, X.; You, X.H.; Yang, Y.; Yuan, D.; Aggoune, H.; Haas, H.; Fletcher, S.; Hepsaydir, E. Cellular architecture and key technologies for 5G wireless communication networks. *IEEE Commun. Mag.* **2014**, *52*, 122–130.
15. Gai, K.; Qiu, M.; Tao, L.; Zhu, Y. Intrusion detection techniques for mobile cloud computing in heterogeneous 5G. *Secur. Commun. Netw.* **2016**, *9*, 3049–3058.
16. Chen, S.; Qin, F.; Hu, B.; Li, X.; Chen, Z. User-centric ultra-dense networks for 5G: Challenges, methodologies, and directions. *IEEE Wirel. Commun.* **2016**, *23*, 78–85.
17. Chatterjee, S.; Kar, A.K.; Gupta, M. Critical Success Factors to Establish 5G Network in Smart Cities: Inputs for Security and Privacy. *J. Glob. Inf. Manag.* **2017**, *25*, 15–37.
18. Eiza, M.H.; Ni, Q.; Shi, Q. Secure and Privacy-Aware Cloud-Assisted Video Reporting Service in 5G-Enabled Vehicular Networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 7868–7881.
19. Yoo, S.G. 5G-VRSec: Secure Video Reporting Service in 5G Enabled Vehicular Networks. *Wirel. Commun. Mob. Comput.* **2017**, *2017*, 7256307.
20. Malhi, A.K.; Batra, S. An efficient certificateless aggregate signature scheme for vehicular ad-hoc networks. *Discrete Math. Theor. Comput. Sci.* **2015**, *17*, 317–338.
21. Horng, S.J.; Tzeng, S.F.; Huang, P.H.; Wang, X.; Li, T.; Khan, M.K. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks. *Inf. Sci.* **2015**, *317*, 48–66.
22. Cho, W.; Park, Y.; Sur, C.; Rhee, K.H. An Improved Privacy-Preserving Navigation Protocol in VANETs. *JoWUA* **2013**, *4*, 80–92.
23. Altayeb, M.; Mahgoub, I. A survey of vehicular ad hoc networks routing protocols. *Int. J. Innov. Appl. Stud.* **2013**, *3*, 829–846.
24. Yin, J.; ElBatt, T.; Yeung, G.; Ryu, B.; Habermas, S.; Krishnan, H.; Talty, T. Performance evaluation of safety applications over DSRC vehicular ad hoc networks. In Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, Philadelphia, PA, USA, 1 October 2004; ACM: New York, NY, USA, 2004; pp. 1–9.
25. Hussain, R.; Son, J.; Eun, H.; Kim, S.; Oh, H. Rethinking vehicular communications: Merging VANET with cloud computing. In Proceedings of the 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom), Taipei, Taiwan, 3–6 December 2012; pp. 606–609.
26. Olariu, S.; Khalil, I.; Abuelela, M. Taking VANET to the clouds. *Int. J. Pervasive Comput. Commun.* **2011**, *7*, 7–21.

27. Hussain, R.; Abbas, F.; Son, J.; Oh, H. TIaaS: Secure cloud-assisted traffic information dissemination in vehicular ad hoc networks. In Proceedings of the 2013 13th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), Delft, The Netherlands, 13–16 May 2013; pp. 178–179.
28. He, W.; Yan, G.; Xu, L.D. Developing vehicular data cloud services in the IoT environment. *IEEE Trans. Ind. Inform.* **2014**, *10*, 1587–1595.
29. Lee, E.; Lee, E.K.; Gerla, M.; Oh, S.Y. Vehicular cloud networking: architecture and design principles. *IEEE Commun. Mag.* **2014**, *52*, 148–155.
30. Nkenyereye, L.; Rhee, K.H. Secure Traffic Data Transmission Protocol for Vehicular Cloud. In *Advances in Computer Science and Ubiquitous Computing*; Springer: Berlin, Germany, 2015; pp. 497–503.
31. Nkenyereye, L.; Tama, B.A.; Park, Y.; Rhee, K.H. A Fine-Grained Privacy Preserving Protocol over Attribute Based Access Control for VANETs. *JoWUA* **2015**, *6*, 98–112.
32. Nkenyereye, L.; Rhee, K.H. Secure Taxi Service Scheme in Vehicular Cloud Environment. *Int. Inf. Inst. (Tokyo) Inf.* **2015**, *18*, 3495.
33. Zhang, N.; Cheng, N.; Gamage, A.T.; Zhang, K.; Mark, J.W.; Shen, X. Cloud assisted HetNets toward 5G wireless networks. *IEEE Commun. Mag.* **2015**, *53*, 59–65.
34. Trivisonno, R.; Guerzoni, R.; Vaishnavi, I.; Soldani, D. SDN-based 5G mobile networks: Architecture, functions, procedures and backward compatibility. *Trans. Emerg. Telecommun. Technol.* **2015**, *26*, 82–92.
35. Mantas, G.; Komninos, N.; Rodriuez, J.; Logota, E.; Marques, H. Security for 5G communications. In *Fundamentals of 5G Mobile Networks*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2015.
36. Yang, N.; Wang, L.; Geraci, G.; Elkashlan, M.; Yuan, J.; Di Renzo, M. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Commun. Mag.* **2015**, *53*, 20–27.
37. Alam, M.; Yang, D.; Rodriguez, J.; Abd-alhameed, R. Secure device-to-device communication in LTE-A. *IEEE Commun. Mag.* **2014**, *52*, 66–73.
38. Lin, X.; Sun, X.; Ho, P.H.; Shen, X. GSIS: A secure and privacy-preserving protocol for vehicular communications. *IEEE Trans. Veh. Technol.* **2007**, *56*, 3442–3456.
39. Raya, M.; Papadimitratos, P.; Aad, I.; Jungels, D.; Hubaux, J.P. Eviction of misbehaving and faulty nodes in vehicular networks. *IEEE J. Sel. Areas Commun.* **2007**, *25*, 1557–1568.
40. Dikaiakos, M.D.; Florides, A.; Nadeem, T.; Iftode, L. Location-aware services over vehicular ad-hoc networks using car-to-car communication. *IEEE J. Sel. Areas Commun.* **2007**, *25*, 1590–1602.
41. Sampigethaya, K.; Li, M.; Huang, L.; Poovendran, R. AMOEBA: Robust location privacy scheme for VANET. *IEEE J. Sel. Areas Commun.* **2007**, *25*, 1569–1589.
42. Chim, T.W.; Yiu, S.; Hui, L.C.; Li, V.O. VSPN: VANET-based secure and privacy-preserving navigation. *IEEE Trans. Comput.* **2014**, *63*, 510–524.
43. Coronado, E.; Cherkaoui, S. Provisioning of on-demand services in vehicular networks. In Proceedings of the Global Telecommunications Conference (GLOBECOM), Honolulu, HI, USA, 30 November–4 December 2009; pp. 1–6.
44. Li, C.T.; Hwang, M.S.; Chu, Y.P. A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. *Comput. Commun.* **2008**, *31*, 2803–2814.
45. Zhu, H.; Lu, R.; Shen, X.; Lin, X. Security in service-oriented vehicular networks. *IEEE Wirel. Commun.* **2009**, *16*, 16–22.
46. Yao, X.; Chen, Z.; Tian, Y. A lightweight attribute-based encryption scheme for the Internet of Things. *Future Gener. Comput. Syst.* **2015**, *49*, 104–112.
47. He, D.; Chen, J.; Zhang, R. An efficient and provably-secure certificateless signature scheme without bilinear pairings. *Int. J. Commun. Syst.* **2012**, *25*, 1432–1442.
48. Chin, W.H.; Fan, Z.; Haines, R. Emerging technologies and research challenges for 5G wireless networks. *IEEE Wirel. Commun.* **2014**, *21*, 106–112.
49. Birem, M.; Berry, F. Dreamcam: A modular fpga-based smart camera architecture. *J. Syst. Archit.* **2014**, *60*, 519–527.
50. Lu, R.; Lin, X.; Zhu, H.; Ho, P.H.; Shen, X. A novel anonymous mutual authentication protocol with provable link-layer location privacy. *IEEE Trans. Veh. Technol.* **2009**, *58*, 1454–1466.
51. Miyaji, A.; Nakabayashi, M.; Takano, S. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2001**, *84*, 1234–1243.

52. Wei, D. Crypto++ Library 5.6.5, a Free C++ Class Library of Cryptographic schemes, 2017. Available online: http://www.cryptopp.com (accessed on 12 May 2017).
53. Demestichas, P.; Georgakopoulos, A.; Karvounas, D.; Tsagkaris, K.; Stavroulaki, V.; Lu, J.; Xiong, C.; Yao, J. 5G on the horizon: Key challenges for the radio-access network. *IEEE Veh. Technol. Mag.* **2013**, *8*, 47–53.
54. Bethencourt, J.; Sahai, A.; Waters, B. Advanced Crypto Software Collection—Ciphertext-Policy Attribute-Based Encryption. Available online: http://acsc.cs.utexas.edu/cpabe/ (accessed on 20 June 2017).
55. MIRACL Crypto SDK; CertiVox UK, R.U. Multiprecision Integer and Rational Arithmetic Cryptographic Library, 2016. Available online: https://www.certivox.com/miracl (accessed on 15 June 2017).
56. Baek, J.; Safavi-Naini, R.; Susilo, W. Public key encryption with keyword search revisited. In Proceedings of the International Conference on Computational Science and Its Applications, Perugia, Italy, 30 June–3 July 2008; pp. 1249–1259.
57. BBCNews. 5G Researchers Manage Record Connection Speed, 2015. Available online: http://www.bbc.co.uk/news/technology-31622297 (accessed on 10 May 2017).