Hindawi
Wireless Communications and Mobile Computing
Volume 2017, Article ID 7256307, 22 pages
https://doi.org/10.1155/2017/7256307

Research Article

5G-VRSec: Secure Video Reporting Service in 5G Enabled Vehicular Networks

Sang Guun Yoo[1,2]

[1]*Departamento de Ciencias de la Computación, Universidad de las Fuerzas Armadas ESPE, Av. General Rumiñahui s/n, Sangolquí, Ecuador*
[2]*Facultad de Ingeniería de Sistemas, Escuela Politécnica Nacional, Ladrón de Guevara E11-253, Quito, Ecuador*

Correspondence should be addressed to Sang Guun Yoo; yysang@espe.edu.ec

Received 25 January 2017; Revised 16 April 2017; Accepted 27 April 2017; Published 25 July 2017

Academic Editor: Oscar Esparza

Despite an imminent arrival of the 5G communication technology, there are only a few research works done using such technology in the field of vehicular networks. One of the pioneers in proposing a service for 5G enabled vehicular networks is the Eiza-Ni-Shi Scheme. In such scheme, the authors present an innovative system model for 5G vehicular networks that enables a secure real-time video reporting service with privacy awareness. Even though the proposed service is very important since it aims to improve the road safety, it cannot be considered secure enough. This work found that the scheme has serious security flaws and functionality limitations. First, it is vulnerable to Department of Motor Vehicles and Law Enforcement Agency impersonation attacks, it allows forged video upload, there is no separation of responsibilities between Law Enforcement Agency and trusted authority, and it is susceptible to privileged insider attack. In addition, it does not contemplate the management of multiple geographic/administrative regions (multiple trusted authorities) which is important in real implementations. In this situation, the present work proposes an extended scheme that eliminates the identified security flaws and implements new features that make the implementation across several geographic/administrative regions possible.

1. Introduction

The 5G communication technology has been one of the most important research fields in the academy over the last several years [1–3], and it also has received the interest of the telecommunication industry worldwide [4–6]. 5G technology is expected to transform the way users communicate by supporting traditional and novel applications that demand high-speed wireless connections with lower latency and promoting both spectrum and energy efficiency [5]. 5G will also give the foundational infrastructure for building a fully realized Internet of Things and Smart Cities and it will allow the implementation of new real-time services.

Despite an imminent arrival of the 5G communication technology, there are only a few research works done using such technology in the field of vehicular networks. One of the pioneers in proposing a service for 5G enabled vehicular networks is [7] (called Eiza-Ni-Shi Scheme in this paper). In such work, the authors propose an innovative system model for 5G vehicular networks that enables a secure real-time video reporting service with privacy awareness, and they indicate that their approach is the first study that visualizes the architecture of 5G enabled vehicular network and solves the security and privacy issues of video reporting services. The Eiza-Ni-Shi Scheme utilizes several previous works to provide a novel scheme for a 5G enabled vehicular network that enables a secure and privacy-aware real-time video reporting service that allows registered vehicles to rapidly deliver the video of accidents to receive an opportune response from official vehicles (e.g., police vehicles or ambulance).

Even though the proposed service is very important contribution since it aims to improve the road safety and therefore save more lives, it cannot be considered secure enough. This work found that the scheme has serious security flaws and functionality limitations. First, it is vulnerable to Department of Motor Vehicles and Law Enforcement Agency (LEA) impersonation attacks, it allows forged video upload, there is no separation of responsibilities between LEA and

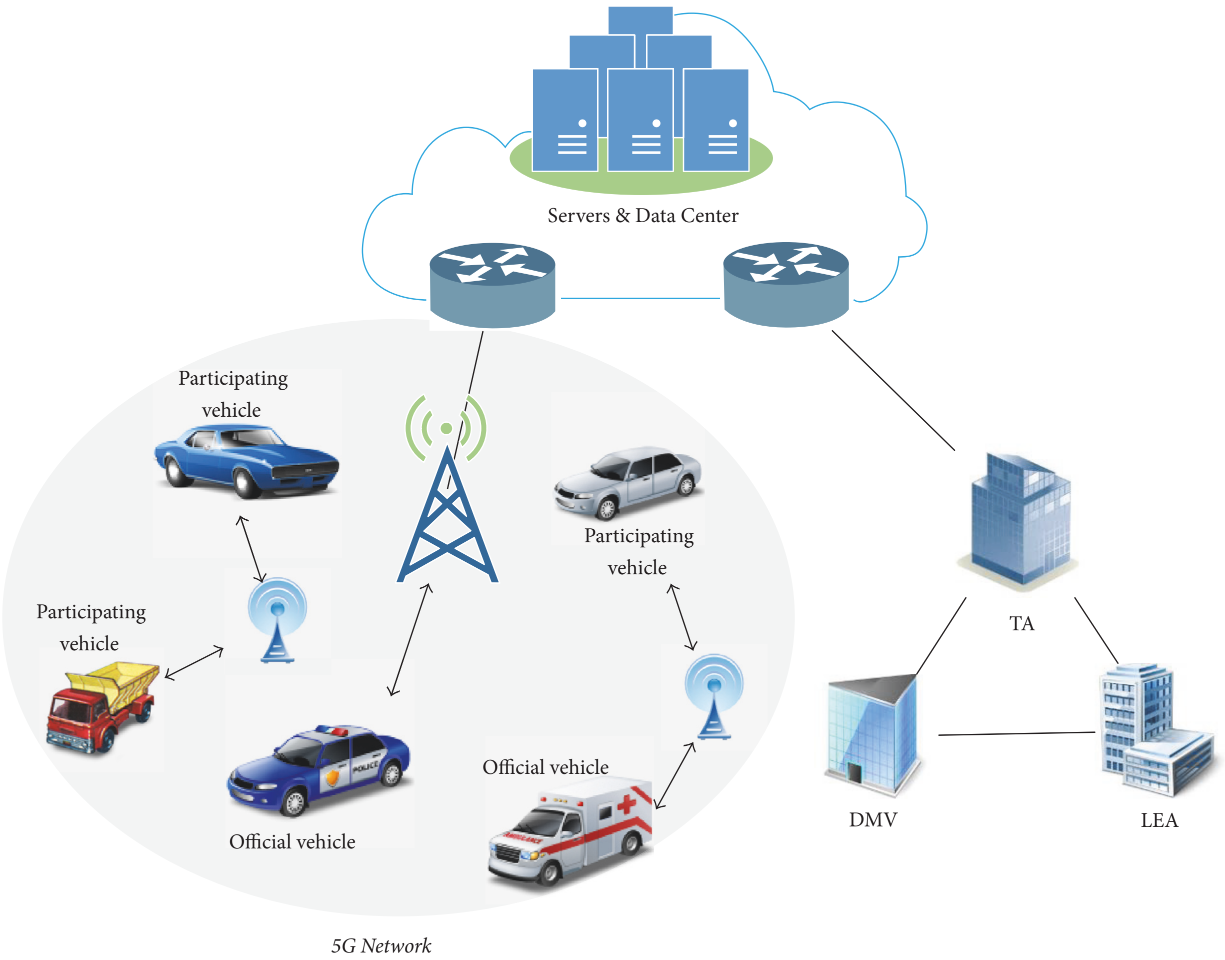


Figure 1: System model of Eiza-Ni-Shi Scheme.

trusted authority, and privileged insider attack is possible in LEA. Additionally, it does not contemplate the management of multiple geographic/administrative regions (see Figure 1) which is important in real implementations. In most of the cases, not all the motorized vehicles are controlled by a centralized entity, but they are delegated to regional entities (e.g., managed per states, cities, or districts). For this reason, the proposed scheme assumes a real world scenario with multiple trusted authorities (TA), Department of Motor Vehicles (DMV), LEAs connected to its own Cloud Platform (see Figure 2).

The intention of this paper is to continue with the research made in [7] by eliminating its security flaws and extending its functionality, that is, making it possible to be implemented across several geographic/administrative regions. The new contributions of this paper are as follows. (1) First, this paper makes a cryptanalysis and functionally analysis of Eiza-Ni-Shi Scheme and demonstrates how it is vulnerable to DMV and LEA impersonation attacks, how it allows forged video upload, that there is no separation of responsibilities between LEA and TA, how privileged insider attack is possible in LEA, and how it does not contemplate the management of multiple geographic/administrative regions (multiple trusted authorities) which is very important in large scale implementations. (2) Secondly, this work develops an improved scheme that delivers a trusted and reliable real-time video reporting service in 5G enabled vehicular networks which solves the identified security flaws. (3) Finally, the proposed design extends the functionality of the service for multiple trusted authorities, Department of Motor Vehicles, Law Enforcement Agencies, and Cloud Platforms which was proposed as future works in [7].

The rest of the paper is organized as follows. Section 2 overviews the preliminary concepts used in both Eiza-Ni-Shi Scheme and the proposed solution. Section 3 then reviews the Eiza-Ni-Shi Scheme and executes its cryptanalysis and functionality analysis. Later, Section 4 presents the extended system model of 5G enabled vehicular network and details the proposed secure and privacy-aware scheme. Section 4 also analyzes the proposed protocol in terms of performance and security. Finally, Section 5 concludes the present paper.

2. Preliminaries

This section introduces the cryptographic meanings used in both Eiza-Ni-Shi Scheme and the proposed scheme.

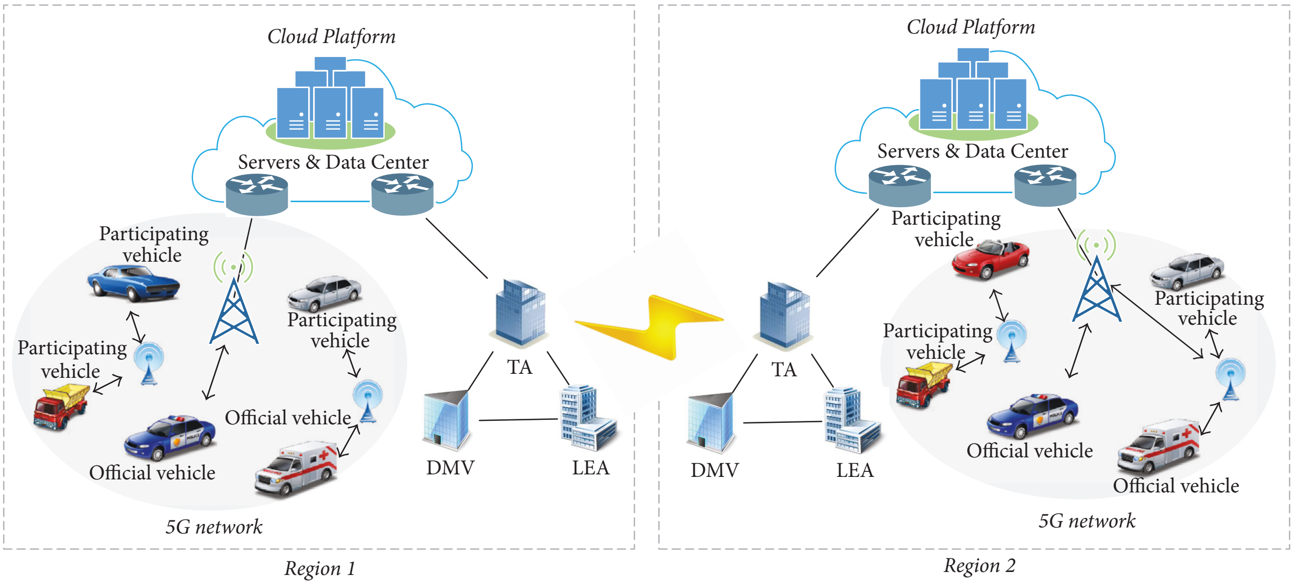


FIGURE 2: Extended system model for secure video reporting service in 5G enabled vehicular network.

2.1. Pseudonymous Authentication Scheme. Let $(G_1, +)$ and $(G_2, +)$ be two cyclic groups of prime order q and $e : G_1 \times G_1 \rightarrow G_2$ be an efficient admissible bilinear map. The TA selects a random generator $P \in G_1$, two hash functions $h(\cdot)$ and $f(\cdot) : \{0,1\}^* \rightarrow G_1$ and a random key $S \in Z^*{}_q$. Then, the TA calculates its public key P_{pub} as $P_{\text{pub}} = sP$ and distributes the parameters $(G_1, G_2, q, P, e, P_{\text{pub}}, h(\cdot), f(\cdot), \text{SEnc}(\cdot), \Delta T)$ where $\text{SEnc}(\cdot)$ is a symmetric encryption function and ΔT is the expiration threshold of a pseudonymous certificate. As well as the Eiza-Ni-Shi Scheme, the proposed solution also uses PASS (pseudonymous authentication scheme with strong privacy preservation) [8] to anonymously authenticate participating vehicles. Applying the concept proposed in [8], the trusted authority generates a private key SK_{TA} and uses it to issue a set of pseudonymous certificates to those vehicles which expressed their willingness to participate in the video reporting service. The size of each pseudonymous certificate is 66 bytes: 21 bytes for the public key, 20 bytes for pseudo-identity, 4 bytes for the validity period, and 21 bytes for digital signature. Finally, the TA generates the private key set corresponding to the pseudonymous certificates and delivers it accompanied with the set of pseudonymous certificates to the participating vehicle and stores the mapping relationship between the real identity of participating vehicle and its pseudo-identities.

2.2. Public Key Encryption with Keyword Search. The Public Key Encryption with Keyword Search (PEKS) is an asymmetric cryptographic mechanism that allows an entity to delegate the storage of its encrypted data, while preserving the capability to search encrypted keywords related to the encrypted information [9, 10]. The entity uses the public key of a recipient R PK_R to calculate the searchable encryption SPEKS of a set of keywords $\text{kw} = \{\text{kw}_1, \text{kw}_2, \ldots, \text{kw}_n\}$ by executing $\text{SPEKS} = \text{PEKS}(\text{PK}_R, \text{kw})$ and uploads the calculated value attached to the encrypted data to the storage server. Later, when search of a keyword is required, the entity creates a trapdoor Tkw_i by executing $\text{Tkw}_i = \text{Trapdoor}(\text{SK}_R, \text{kw}_i)$, where SK_R is the private key of the recipient R and kw_i is the keyword used for search. Following this, the storage server uses Tkw_i to execute the search process by executing $\text{Test}(\text{SPEKS}, \text{Tkw}_i)$. The search process will return true if $\text{kw}_i \in \text{kw}$. Finally, the encrypted data associated with kw_i is returned for decryption.

2.3. Ciphertext-Policy Attribute Based Encryption. Ciphertext-Policy Attribute Based Encryption (CP-ABE or simply ABE) is an asymmetric cryptographic system for realizing complex access control on encrypted data [11]. The data to be protected is encrypted using a public key in association with a specific policy. The encrypted data is accessible only by those users who have the decryption key and have the attributes that satisfy the policy specified during the encryption process. Based on [7], it is possible to use as attributes the following values {"police vehicle", "ambulance", "traffic authority", "traffic law enforcement"}. In the phase of system initialization, the TA generates a public key PK_{ABE} and a master key MK_{ABE}. The MK_{ABE} is utilized to generate a decryption key for a specific entity E that is associated with a set of attributes (AS) that describes E, *for example*, AS = {"police vehicle", "traffic authority", "traffic law enforcement"}. In order to give E an access to the encrypted data, it should be encrypted using a specific policy, *Policy*, *for example*, policy = {"police vehicle" OR "traffic authority"}, as $\text{ABEC} = \text{ABE.Enc}(\text{PK}_{\text{ABE}}, \text{data}, \text{Policy})$. Thus, E can access the encrypted data and decrypts it as follows: $\text{data} = \text{ABE.Dec}(\text{ABEC}, \text{decryption key})$.

3. Review and Cryptanalysis of Eiza-Ni-Shi Scheme

This section reviews the scheme proposed in [7]. This section also cryptanalyses its features to demonstrate how it is vulnerable to DMV and LEA impersonation attacks, how it allows forged video upload, that there is no separation of responsibilities between LEA and TA, how privileged insider attack is possible in LEA, and how it does not contemplate the management of multiple geographic/administrative regions (multiple trusted authorities) which is very important in large scale implementations.

3.1. Review of Eiza-Ni-Shi Scheme. Figure 1 shows the system model proposed by the Eiza-Ni-Shi Scheme. The main entities are the Department of Motor Vehicles (DMV), trusted authority (TA), Law Enforcement Agency (LEA), Cloud Platform, and Vehicles (participating vehicles and official vehicles). In the following, there is the brief explanation of different entities that participate in the scheme.

Cloud Platform. The Cloud Platform provides the functionality of data storage. Being more concrete, it stores the videos of traffic accidents generated by the reporting service. Obviously, since the Cloud Platform is connected to the Internet, it will be accessible anywhere. It is important to indicate that the reported videos are not delivered directly to the authorities since the communication route to the recipient may not be available; that is, the official vehicle is not reachable via multihop communication. The scheme assumes the availability of a reliable multipath routing algorithm (such as [12]) to find stable routes to the Cloud Platform. In addition, it is assumed that vehicles use the 5G communication technology to access the Cloud Platform.

Trusted Authority (TA). This is the entity that manages the pseudonymous certificates, certificates and secret keys of participating vehicles and official vehicles. The Eiza-Ni-Shi Scheme assumes that TA is secure and it is trusted by all the other entities of the 5G enabled vehicular network system.

Department of Motor Vehicles (DMV). All vehicles are registered periodically in the DMV. Besides the traditional identifier of the vehicle, *that is*, Electronic License Plate or Electronic Chassis Number, each vehicle is assumed to have a unique but not fixed 5G identifier. It means the 5G identified can be modified in each inspection of the vehicle by DMV.

Law Enforcement Agency (LEA). LEA is integrated part of the system since the reported information, that is, coordinate of accident and video of the accident, is very sensitive information.

Participant Vehicles. These are those vehicles that are participating in the cloud-assisted video reporting service. Special equipment (a small computer with video camera, sensors, and 5G communication) is installed in the participant vehicles. The vehicles will record the video and such video will be uploaded to the Cloud Platform when an accident is detected.

Official Vehicles. Official Vehicles are those vehicles that are designated and authorized to respond to a traffic accident (e.g., police vehicle or ambulance). These vehicles are usually operated by designated agencies part of the government but also sometimes run by nongovernmental organizations and some private companies.

The Eiza-Ni-Shi Scheme proposes a protocol composed of 4 phases called (1) system initialization, (2) participants and official vehicles registration, (3) video transmission, and (4) video receipt/retrieval. The notations used in Eiza-Ni-Shi Scheme are detailed in (i) in the Notations.

3.1.1. System Initialization. The trusted authority (TA) manages a specific area that could be a state, province, or district. The TA chooses a validity period threshold of a pseudonymous certificate ΔT and estimates the number of pseudonymous certificates that a vehicle needs to acquire. It is assumed that the issued pseudonymous certificates (stored in each vehicle) cannot be used to impersonate other vehicles because each certificate has a specific validity period and the number of certificates is relatively small.

3.1.2. Participants and Official Vehicles Registration. The participant vehicles are registered executing the following steps.

Step 1. During the vehicles' annual inspection, the user indicates his/her disposition to use the service. Then, the vehicle registers its identity C_v, unique 5G identity 5G_ID, and $\mathrm{PKE}(P_{\mathrm{pub}}, S_r)$ with the Department of Motor Vehicles (DMV), where S_r is a random symmetric key $s_r \in Z^*{}_q$, P_{pub} is TA's public key, and $\mathrm{PKE}(\cdot)$ is an asymmetric encryption function.

Step 2. The DMV registers the data of the participant vehicle in its database and forwards $\{\text{5G\_ID}, \mathrm{PKE}(P_{\mathrm{pub}}, S_r)\}$ to the TA requesting the issue of pseudonymous certificates for the vehicle.

Step 3. Upon receiving the request from DMV, the TA creates a set of pseudonymous certificates $\{\mathrm{PCert}_{\mathrm{TA,5G\_ID},j}\}$, a set of private keys $\{\mathrm{SK}_{\mathrm{5G\_ID},j}\}$, a policy, *Policy* = {"police vehicle" OR "ambulance" OR "traffic law enforcement" OR "traffic authority"}, and a tag $U \in Z^*{}_q$, and delivers them to the DMV by sending $\mathrm{SEnc}(S_r, (\{\mathrm{SK}_{\mathrm{5G\_ID},j}\}, \{\mathrm{PCert}_{\mathrm{TA,5G\_ID},j}\}, \mathrm{PK}_{\mathrm{ABE}}, \mathrm{Policy}, U))$, where $\mathrm{SEnc}(\cdot)$ is an symmetric encryption function and $\mathrm{PK}_{\mathrm{ABE}}$ is the public key used to encrypt a one-time random encryption key S_{key} under *Policy* using CP-ABE [11]. The tag U is a preagreed value between the TA and the Cloud Platform; such value is used by C_v to tag the traffic accident video when uploaded and it is used by the Cloud Platform to recognize the space to store the received video and to notify the registered official vehicles.

Step 4. The DMV forwards the received information to the vehicle. It is important to note that DMV only manages the mapping between the vehicle's 5G_ID and its real identity C_v and it does not know the issued pseudonymous credentials. On the other hand, the TA manages the mapping between the 5G_ID identity and the corresponding pseudonyms without knowledge of vehicles real identity C_v. This separation of responsibilities creates a more secure environment. Upon receiving the data from DMV, the participating vehicle stores the received information into a tamper-proof device (TPD) that it is equipped with [13, 14].

On the other side, designated official vehicles are registered to receive the notification of reported traffic accident videos. The official vehicles registration is executed with following steps.

Steps 5 and 6. A designated official vehicle DV_i sends a registration request to the TA via the Law Enforcement Agency (LEA).

Steps 7 and 8. After verifying the request, the TA generates and delivers the certificate $\mathrm{Cert}_{\mathrm{TA,DV}i}$ to DV_i and uses the $\mathrm{MK}_{\mathrm{ABE}}$ to create a decryption key $\mathrm{dk}_{\mathrm{AS}}$ associated with a set of attributes such as AS = {"police vehicle", "ambulance", "traffic law enforcement", "traffic authority"}. The attributes will change depending on the type of the official vehicle. The confidential information generated by TA is then delivered to the DV_i's tamper-proof device via LEA.

Step 9. DV_i uses the data received in previous step to register with the Cloud Platform.

3.1.3. Video Transmission. This phase is executed when an accident occurs to the participant vehicle. This phase is executed as follows.

Step 10. The participating vehicle C_v generates a random one-time symmetric key S_{key} and executes $\mathrm{Enc}_C = \mathrm{SEnc}(S_{\mathrm{key}}, \mathrm{TV}_r)$ to encrypt the accident video report TV_r.

Step 11. C_v reads the public key of the recipient R (PK_R) and executes $S_{\mathrm{PEKS}} = \mathrm{PEKS}(\mathrm{PK}_R, \mathrm{kw})$ to generate a searchable encryption of the keywords kw = {"accident video report", location, date and time}.

Step 12. C_v encrypts S_{key} using the CP-ABE function under Policy as follows: $\mathrm{ABE}_C = \mathrm{ABE.Enc}(\mathrm{PK}_{\mathrm{ABE}}, S_{\mathrm{key}}, \mathrm{Policy})$ to allow only official vehicles having $\mathrm{dk}_{\mathrm{AS}}$ with *Policy* to access ABE_C and obtain S_{key}.

Step 13. Using the selected pseudonymous certificate, C_v executes $\sigma_{\mathrm{5G\_ID},j} = \mathrm{Sign}(\mathrm{SK}_{\mathrm{5G\_ID},j}, h(\mathrm{Enc}_C \parallel S_{\mathrm{PEKS}} \parallel \mathrm{ABE}_C \parallel h(U)))$, where $\mathrm{Sign}(\cdot)$ is the signing function, $\mathrm{SK}_{\mathrm{5G\_ID},j}$ is the C_v's private key associated with the selected pseudonymous certificate, and "$\parallel$" denotes data concatenation.

Step 14. C_v uploads $\{\mathrm{Enc}_C, S_{\mathrm{PEKS}}, \mathrm{ABE}_C, h(U), \sigma_{\mathrm{5G\_ID},j}, \mathrm{PCert}_{\mathrm{TA,5G\_ID},j}\}$ to the Cloud Platform over the 5G network.

3.1.4. Video Receipt/Retrieval. This phase is executed when the accident video is uploaded to the Cloud Platform. This phase is executed as follows.

Step 15. First, the Cloud Platform verifies $h(U)$ value and then notifies the accident to the nearest official vehicle DV_i by sending $\{\mathrm{Enc}_C, S_{\mathrm{PEKS}}, \mathrm{ABE}_C, h(U), \sigma_{\mathrm{5G\_ID},}j, \mathrm{PCert}_{\mathrm{TA,5G\_ID},j}\}$. The authors assume that the location information of the official vehicles is updated periodically in the cloud.

Step 16. DV_i verifies the received certificate $\mathrm{PCert}_{\mathrm{TA,5G\_ID},j}$ by executing $\mathrm{Verify}(P_{\mathrm{pub}}, \mathrm{PCert}_{\mathrm{TA,5G\_ID},j}, \sigma_{\mathrm{TA,5G\_ID},j})$, where $\mathrm{Verifiy}(\cdot)$ is a verification function. After verification of authenticity of $\mathrm{PCert}_{\mathrm{TA,5G\_ID}}$, DV_i extracts the public key $\mathrm{PK}_{\mathrm{5G\_ID},j}$ from the pseudonymous certificate.

Step 17. DV_i verifies $\sigma_{\mathrm{5G\_ID},j}$ by executing $\mathrm{Verify}(\mathrm{PK}_{\mathrm{5G\_ID},j}, h(\mathrm{Enc}_C \parallel S_{\mathrm{PEKS}} \parallel \mathrm{ABE}_C \parallel h(U)), \sigma_{\mathrm{5G\_ID},j})$.

Step 18. After verification of authenticity of $\sigma_{\mathrm{5G\_ID},j}$, DV_i executes $S_{\mathrm{key}} = \mathrm{ABE.Dec}(\mathrm{ABE}_C, \mathrm{dk}_{\mathrm{AS}})$ to get the one-time symmetric encryption key, where $\mathrm{ABE.Dec}(\cdot)$ is the CP-ABE decryption function.

Step 19. DV_i executes $\mathrm{TV}_r = \mathrm{SDec}(S_{\mathrm{key}}, \mathrm{Enc}_C)$ and gets the traffic accident video, where $\mathrm{SDec}(\cdot)$ is a symmetric decryption function.

In the Eiza-Ni-Shi Scheme, the encrypted videos are stored on the Cloud Platform to allow access whenever they are needed. In other words, LEA can search for the traffic accident videos on the cloud at any moment.

Step 20. LEA generates the searchable trapdoor token Tkw_i as follows: $\mathrm{Tkw}_i = \mathrm{Trapdoor}(\mathrm{SK}_R, \mathrm{kw}_i)$, where keyword kw_i can be a location, a date, or just "accident video report."

Step 21. LEA sends the generated Tkw_i to the Cloud Platform. The authors assume that there is a secure channel between LEA and Cloud Platform.

Step 22. The receipt of Tkw_i authorizes the search process over the ciphertext at the cloud.

Step 23. LEA receives the message $\{\mathrm{Enc}_C, S_{\mathrm{PEKS}}, \mathrm{ABE}_C, h(U), \sigma_{\mathrm{5G\_ID},j}, \mathrm{PCert}_{\mathrm{TA,5G\_ID},j}\}$. Finally, LEA uses the same procedure to receive the video file TV_r.

3.2. Cryptanalysis and Functionality Analysis of Eiza-Ni-Shi Scheme. This section makes an analysis of the Eiza-Ni-Shi Scheme and shows how it has several security vulnerabilities and a critical functionality limitation.

No Management of Multiple Trusted Authorities. First of all, one of the main limitations of the Eiza-Ni-Shi Scheme is the lack of a mechanism that covers different geographic/administrative regions of vehicular networks. This limitation is mentioned also by the same authors of Eiza-Ni-Shi Scheme and it is left for future work. In most of countries in the world, the control of motorized vehicles is done per different geographic/administrative regions delegating those responsibilities to regional authorities (e.g., state authorities). For this reason, it is necessary to consider a real world scenario with multiples TAs, DMVs, and LEAs connected to its own Cloud Platforms.

DMV Impersonation Attack. The adversary U_a can execute the DMV impersonation attack with the following steps. Since the 5G_ID is not a fixed value and it is not verified by the TA, U_a can generate any random value as 5G_ID. Once 5G_ID is generated, U_a will generate a random symmetric key S_r and will send a registration message $\mathrm{request}(\mathrm{5G\_ID}, \mathrm{PKE}(P_{\mathrm{pub}}, S_r))$ to the TA. Since the 5G_ID is not a fixed value and it is not verified, TA will process the request and it will return the $\mathrm{SEnc}(S_r, (\{\mathrm{SK}_{\mathrm{5G\_ID},j}\}, \{\mathrm{PCert}_{\mathrm{TA,5G\_ID},j}\}, \mathrm{PK}_{\mathrm{ABE}}, \mathrm{Policy}, U))$ message. Since S_r was generated by U_a, he/she will be able to obtain the tuple $\{\{\mathrm{SK}_{\mathrm{5G\_ID},j}\}, \{\mathrm{PCert}_{\mathrm{TA,5G\_ID},j}\}, \mathrm{PK}_{\mathrm{ABE}}, \mathrm{Policy}, U\}$.

Forged Video Upload. By executing the DMV impersonation attack, U_a can obtain the valid private keys $\{\mathrm{SK}_{\mathrm{5G\_ID},j}\}$, pseudonymous certificates $\{\mathrm{PCert}_{\mathrm{TA,5G\_ID},j}\}$, $\mathrm{PK}_{\mathrm{ABE}}$, Policy, and U. With these values, the adversary can simulate a traffic accident by uploading a false video.

Nonseparation of Responsibilities between LEA and TA. Eiza-Ni-Shi Scheme separates the responsibilities between DMV and TA. However, it does not separate the responsibilities between LEA and TA. Following the same reasoning of separation of responsibilities between DMV and TA, the mapping between the official vehicle real identity DV_i and its 5G_ID should be managed only by LEA and not by TA.

Privileged Insider Attack in LEA. Since LEA receives $\mathrm{Cert}_{\mathrm{TA,DV}i}$ and $\mathrm{dk}_{\mathrm{AS}}$ of each official vehicle in plaintext, the privileged insider of LEA could store such values. Therefore, privileged insider could access every traffic accident video impersonating official vehicles.

LEA Impersonation Attack. Since the 5G_ID is not a fixed value and it is not verified by the TA, U_a can generate any random value as 5G_ID. Once 5G_ID is generated, U_a will generate a random symmetric key S_r and will send a registration request message $\mathrm{request}(\mathrm{DV}_i, \mathrm{5G\_ID})$ to the TA. Since the $\{\mathrm{DV}_i, \mathrm{5G\_ID}\}$ tuple is not verified by TA, TA will process the request and it will return $\mathrm{Cert}_{\mathrm{TA,DV}i}$ and $\mathrm{dk}_{\mathrm{AS}}$ message.

Exposure of Location of Official Vehicles. The authors of Eiza-Ni-Shi Scheme assume that the location data of official vehicles are delivered periodically to the Cloud Platform in plaintext. The exposure of such data (e.g., localization of police vehicles) could be a critical problem since criminals could use such information to perform illegal activities. The authors of Eiza-Ni-Shi Scheme admit this limitation in their paper and propose a solution for it as a future work.

4. 5G-VRSec: The Proposed Secure Video Reporting Service in 5G Enabled Vehicular Networks

This section describes the details of the proposed solution. The proposed scheme eliminates the security flaws shown in previous section and incorporates the concept of different geographic/administrative regions involving several TAs, DMVs, LEAs, and Cloud Platforms (see Figure 2).

4.1. System Model.

4.1. System Model. The proposed scheme uses the 5G mobile network as the foundational communication technology. 5G technology was selected for the vehicular network because of its high speed and capacity required to upload and download the traffic accident videos in real time.

Figure 2 shows the proposed multiregional and multitier 5G enabled vehicular network. The proposed scheme makes the management of different geographic/administrative regions responding to the real world needs possible. Since most of the countries in the world control the motorized vehicles through regional authorities (e.g., state authorities), the proposed scheme assumes a more realistic world scenario with multiple TAs, DMVs, and LEAs connected to its own Cloud Platform. In other words, the proposed scheme provides a solution to the limitation left as future work in [7].

Each geographical or administrative region is composed of its own Department of Motor Vehicles (DMV), trusted authority (TA), Law Enforcement Agency (LEA), Cloud Platform, and vehicles (participating vehicles and official vehicles). Since the proposed solution allows multiple geographical or administrative regions, there are additional considerations to bear in mind: (1) The implementation of the Cloud Platform can be unique for the complete system (nationwide), or it can be independent for each geographic/administrative region; it will depend on local laws and regulations. Obviously, since the Cloud Platform is connected to the Internet, a Cloud Platform of a region will be accessible from other regions. And (2) the proposed scheme assumes that TA is secure and it is trusted by all the other entities of the 5G enabled vehicular network system of the same geographical/administrative region. Additionally, we assume that a TA of a region is trusted by other TAs located in other geographical/administrative regions.

4.2. Design Criteria: System Considerations and Assumptions. This section describes the security criteria and assumptions used in designing the proposed scheme.

Confidentiality and Integrity. Messages containing secret data transmitted and received by entities must be protected from malicious users. Additionally, unauthorized alterations of confidential data must be identified by the proposed service.

Protection against Untrusted Communications. The communication among TAs, DMVs, and LEAs (messages coming from the mentioned entities) is not fully trusted since privileged insider attack could be executed. Therefore, the protection of confidential messages using cryptographic algorithms is necessary.

Insecure Channels. Most of communication channels are considered insecure. This means that sniffing and spoofing of messages can occur in such channels. The following communication channels are considered insecure.

(i) The communication channel between DV_i and Cloud Platform is not secure.

(ii) The communication channel between DV_i and LEA is not secure.

(iii) The communication channel between C_v and TA is not secure.

(iv) The communication channel between C_v and Cloud Platform is not secure.

(v) The communication channel between LEA and Cloud Platform is not secure.

(vi) The communication channel between TA and ATA is not secure.

Secure Channel. Only one communication channel is considered secure, that is, communication between C_v and DMV. The mentioned communication channel is considered secure because the communication is executed face to face. It means that the owner of C_v must visit the DMV's office to register his vehicle.

Trusted Entities. The servers managed by different entities, that is, DMVs, LEAs, TAs, and Cloud Platforms, are managed by trusted service providers. Therefore, such infrastructures are considered secure, and their security is not considered as part of this paper.

Authentication and Nonrepudiation. Each participating vehicle C_v must authenticate to the Cloud Platform to upload the reporting video, and it cannot repudiate later the execution of video uploading process.

Cryptographic Keys. We assume that each entity, that is, TA, DMV, LEA, and Cloud Platform, has its own asymmetric key pair and they are administered securely using existing algorithms.

Security against Common Attacks. The proposed solution must be strong against the most common attacks such as replay attack, privileged insider attack, impersonation attack, and message sniffing/spoofing.

Secure Storage. The proposed scheme assumes that the participating vehicles C_v and designated official vehicles DV_i have a tamper-proof device for storage and management of confidential data (e.g., keys and pseudonymous certificates). Security technologies such as TrustZone by ARM [13] and Secure RAM by Freescale [14] could be possible solutions for the mentioned tamper-proof devices.

Separation of Responsibilities among DMV, LEA, and TA. Even though DMV, LEA, and *TA* are trusted entities, it is important to make a separation of responsibilities making each of the entities see and store information related to its jurisdiction. The separation of responsibilities increases the level of security and privacy of users.

4.3. Protocols.

The proposed scheme includes eight different phases called (1) system initialization, (2) participant vehicles registration, (3) official vehicles registration, (4) participation vehicle handover, (5) video transmission, (6) video search, (7) Pseudo-Certificate Revocation, and (8) interregion certificate revocation. The notations used in the proposed protocol differ a little bit from the ones used in Eiza-Ni-Shi Scheme since the proposed scheme covers wider functionalities and requires new notations. The mentioned notations are detailed in (ii) in the Notations.

4.3.1. System Initialization.

In the proposed system, each trusted authority (TA) manages a certain geographic/administrative regional area (e.g., a state, province, or district). All the trusted authorities share the same ΔT, which indicates the validity period threshold of a pseudonymous certificate issued to a participating vehicle. It is important to notice that having the same ΔT in each trusted authority does not mean synchronization among those entities; it just means that all TAs must store the same value of ΔT as a constant when the service is implemented. Since the value of ΔT is defined as a governmental regulation for this service, the value of ΔT is not modified after implementation. If the governmental regulation for the services is modified, the TA's administrator must modify manually the value of ΔT. On the other hand, it is important to remember that each pseudonymous certificate is usable only once and it has an expiration time which is equal to $\mathrm{LastPCertTime}_{Cv} + \Delta T$, where $\mathrm{LastPCertTime}_{Cv}$ is the last time where a pseudonymous certificate of a specific participating vehicle C_v was used.

Since each pseudonymous certificate has an expiration time, the TA must estimate the number of certificates to be issued to each C_v. We also think it is a good idea to issue enough pseudonymous certificates for a year, until the next vehicle inspection. For example, if $\Delta T = 1$ hour, the number of pseudonymous certificates required for a C_v during a year will be $24 \times 365 = 8760$. Considering that the certificate size is 66 bytes (as indicated in Section 2), the total amount of space required will be approximately 565 KB, which is a reasonable overhead in terms of storage. As mentioned in Section 4.2., we assume that each C_v has a tamper-proof device for storage and management of confidential data (e.g., keys and pseudonymous certificates).

4.3.2. Participant Vehicle Registration Protocol.

This protocol is executed during the annual vehicle inspection or whenever a user expresses his/her willingness to participate in the video reporting service. This protocol is composed of the following steps (see Figure 3).

A participant vehicle generates a random symmetric key $s_{r1} \in Z^*{}_q$ and sends $\{C_v, \mathrm{5G\_ID}_{Cv}, \mathrm{PKE}(\mathrm{PK}_{\mathrm{TA}}, S_{r1})\}$ to the Department of Motor Vehicles (DMV), where C_v is the unique identification of the participating vehicle, $\mathrm{5G\_ID}_{Cv}$ is the 5G identification of the vehicle, $\mathrm{PK}_{\mathrm{TA}}$ is the public key of the trusted authority (TA) of the region which the participant vehicle is part of, and $\mathrm{PKE}(x, y)$ is the public key encryption function of message y using key x.

Once the message is received, DMV verifies physically the correctness of the C_v, then gets its current timestamp TS', and creates the message $M1 = \{\mathrm{5G\_ID}_{Cv}, \mathrm{TS}', \mathrm{PKE}(\mathrm{PK}_{\mathrm{TA}}, S_{r1})\}$. Upon generation of $M1$, DMV signs $M1$ using its private key

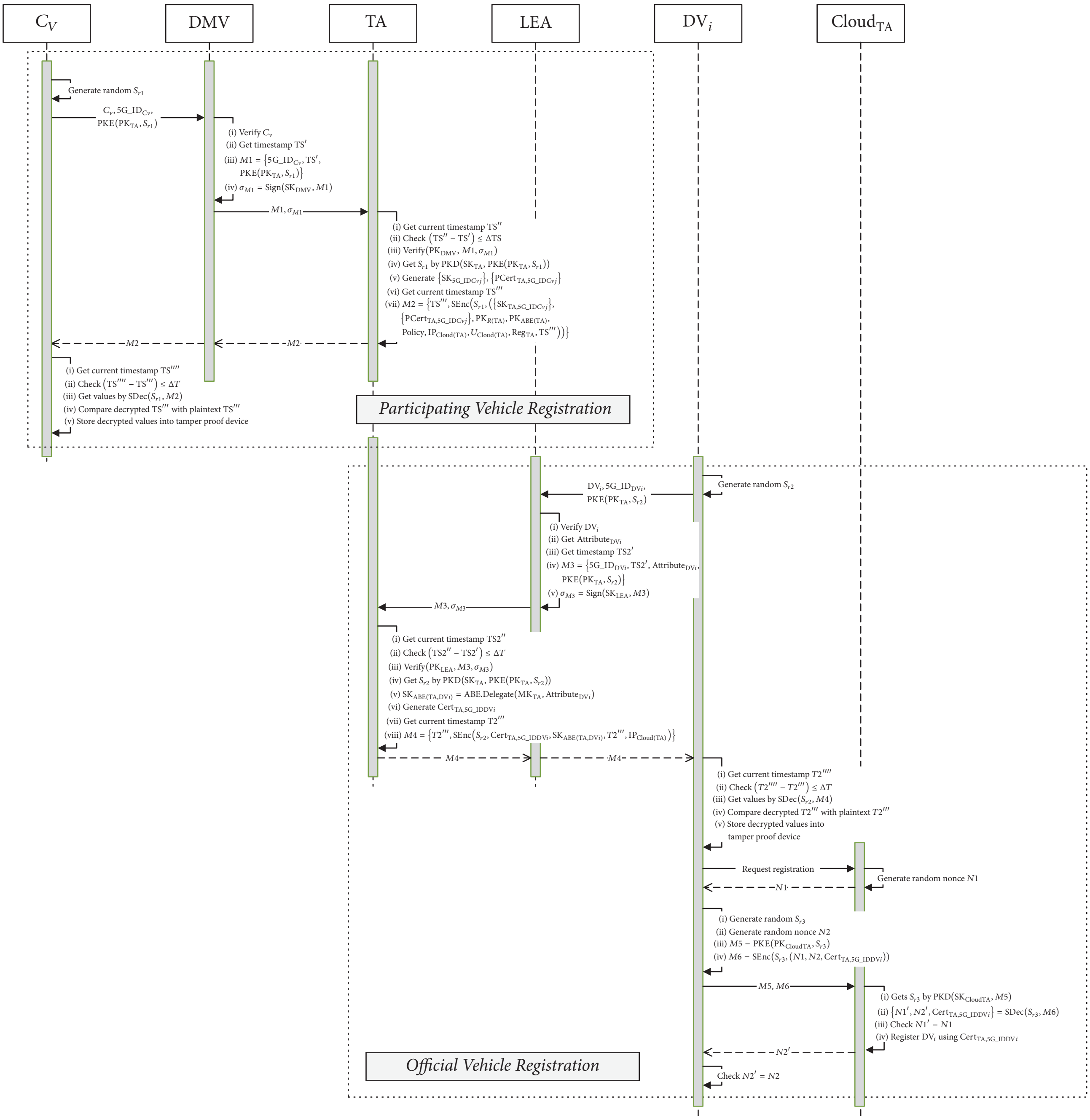

C_V
DMV
TA
LEA
DV_i
$\mathrm{Cloud}_{\mathrm{TA}}$
Generate random S_{r1}
C_v, 5G_ID$_{Cv}$, PKE(PK$_{\mathrm{TA}}$, S_{r1})
(i) Verify C_v
(ii) Get timestamp TS$'$
(iii) $M1 = \{$5G_ID$_{Cv}$, TS$'$, PKE(PK$_{\mathrm{TA}}$, S_{r1})$\}$
(iv) σ_{M1} = Sign(SK$_{\mathrm{DMV}}$, $M1$)
$M1, \sigma_{M1}$
(i) Get current timestamp TS$''$
(ii) Check (TS$''$ − TS$'$) ≤ ΔTS
(iii) Verify(PK$_{\mathrm{DMV}}$, $M1$, σ_{M1})
(iv) Get S_{r1} by PKD(SK$_{\mathrm{TA}}$, PKE(PK$_{\mathrm{TA}}$, S_{r1}))
(v) Generate $\{$SK$_{5G\_IDCvj}\}$, $\{$PCert$_{TA,5G\_IDCvj}\}$
(vi) Get current timestamp TS$'''$
(vii) $M2 = \{$TS$'''$, SEnc(S_{r1}, ($\{$SK$_{TA,5G\_IDCvj}\}$, $\{$PCert$_{TA,5G\_IDCvj}\}$, PK$_{R(\mathrm{TA})}$, PK$_{\mathrm{ABE(TA)}}$, Policy, IP$_{\mathrm{Cloud(TA)}}$, $U_{\mathrm{Cloud(TA)}}$, Reg$_{\mathrm{TA}}$, TS$'''$))$\}$
$M2$
$M2$
(i) Get current timestamp TS$''''$
(ii) Check (TS$''''$ − TS$'''$) ≤ ΔT
(iii) Get values by SDec(S_{r1}, $M2$)
(iv) Compare decrypted TS$'''$ with plaintext TS$'''$
(v) Store decrypted values into tamper proof device
Participating Vehicle Registration
Generate random S_{r2}
DV$_i$, 5G_ID$_{\mathrm{DV}i}$, PKE(PK$_{\mathrm{TA}}$, S_{r2})
(i) Verify DV$_i$
(ii) Get Attribute$_{\mathrm{DV}i}$
(iii) Get timestamp TS2$'$
(iv) $M3 = \{$5G_ID$_{\mathrm{DV}i}$, TS2$'$, Attribute$_{\mathrm{DV}i}$, PKE(PK$_{\mathrm{TA}}$, S_{r2})$\}$
(v) σ_{M3} = Sign(SK$_{\mathrm{LEA}}$, $M3$)
$M3, \sigma_{M3}$
(i) Get current timestamp TS2$''$
(ii) Check (TS2$''$ − TS2$'$) ≤ ΔT
(iii) Verify(PK$_{\mathrm{LEA}}$, $M3$, σ_{M3})
(iv) Get S_{r2} by PKD(SK$_{\mathrm{TA}}$, PKE(PK$_{\mathrm{TA}}$, S_{r2}))
(v) SK$_{\mathrm{ABE(TA,DV}i)}$ = ABE.Delegate(MK$_{\mathrm{TA}}$, Attribute$_{\mathrm{DV}i}$)
(vi) Generate Cert$_{TA,5G\_IDDVi}$
(vii) Get current timestamp T2$'''$
(viii) $M4 = \{T2'''$, SEnc(S_{r2}, Cert$_{TA,5G\_IDDVi}$, SK$_{\mathrm{ABE(TA,DV}i)}$, $T2'''$, IP$_{\mathrm{Cloud(TA)}}$)$\}$
$M4$
$M4$
(i) Get current timestamp $T2''''$
(ii) Check ($T2''''$ − $T2'''$) ≤ ΔT
(iii) Get values by SDec(S_{r2}, $M4$)
(iv) Compare decrypted $T2'''$ with plaintext $T2'''$
(v) Store decrypted values into tamper proof device
Request registration
Generate random nonce $N1$
$N1$
(i) Generate random S_{r3}
(ii) Generate random nonce $N2$
(iii) $M5$ = PKE(PK$_{\mathrm{CloudTA}}$, S_{r3})
(iv) $M6$ = SEnc(S_{r3}, ($N1$, $N2$, Cert$_{TA,5G\_IDDVi}$))
$M5$, $M6$
(i) Gets S_{r3} by PKD(SK$_{\mathrm{CloudTA}}$, $M5$)
(ii) $\{N1'$, $N2'$, Cert$_{TA,5G\_IDDVi}\}$ = SDec(S_{r3}, $M6$)
(iii) Check $N1' = N1$
(iv) Register DV$_i$ using Cert$_{TA,5G\_IDDVi}$
$N2'$
Check $N2' = N2$
Official Vehicle Registration

Figure 3: Participating and Official Vehicle Registrations.

$\mathrm{SK}_{\mathrm{DMV}}$ by executing $\sigma_{M1} = \mathrm{Sign}(\mathrm{SK}_{\mathrm{DMV}}, M1)$. Finally, DMV sends $M1$ and σ_{M1} to TA.

Upon receiving the message, TA verifies the freshness of the message by checking the fulfillment of $(\mathrm{TS}''-\mathrm{TS}') \leq \Delta\mathrm{TS}$, where TS'' is the current timestamp of TA and $\Delta\mathrm{TS}$ is the timestamp expiration threshold. Only if the message is fresh, the TA verifies the authenticity of the received signature σ_{M1} as follows: $\mathrm{Verify}(\mathrm{PK}_{\mathrm{DMV}}, M1, \sigma_{M1})$. After signature verification, TA obtains S_{r1} by executing $\mathrm{PKD}(\mathrm{SK}_{\mathrm{TA}}, \mathrm{PKE}(\mathrm{PK}_{\mathrm{TA}}, S_{r1}))$ and then generates the set of private keys $\{\mathrm{SK}_{\mathrm{TA,5G\_IDC}vj}\}$ and a set of pseudonymous certificates $\{\mathrm{PCert}_{\mathrm{TA,5G\_IDC}vj}\}$ corresponding to $\mathrm{5G\_ID}_{Cv}$, where $\mathrm{PKD}(x, y)$ is the public key decryption function of message y using key x. After that, TA returns the message $M2 = \{\mathrm{TS}''', \mathrm{SEnc}(S_{r1},(\{\mathrm{SK}_{\mathrm{TA,5G\_IDC}vj}\}, \{\mathrm{PCert}_{\mathrm{TA,5G\_IDC}vj}\}, \mathrm{PK}_{R(\mathrm{TA})}, \mathrm{PK}_{\mathrm{ABE(TA)}}, \mathrm{Policy}, \mathrm{IP}_{\mathrm{Cloud(TA)}}, U_{\mathrm{Cloud(TA)}}, \mathrm{Reg}_{\mathrm{TA}}, \mathrm{TS}'''))\}$ to DMV, where $\mathrm{PK}_{R(\mathrm{TA})}$ is the public key of TA for Public Key Encryption with Keyword Search, $\mathrm{PK}_{\mathrm{ABE(TA)}}$ is the public key of TA for the Attributed Based Encryption, *Policy* is the access policy of traffic accident videos uploaded by C_v (e.g., Policy = {"police vehicle" OR "ambulance" OR "traffic law enforcement" OR "traffic authority"}), $\mathrm{IP}_{\mathrm{Cloud(TA)}}$ is the IP address of the Cloud Platform of TA, $U_{\text{Cloud(TA)}} \in Z^{*}{}_{q}$ is the a tag preagreed upon between TA and the Cloud Platform of TA (Cloud_{TA}), Reg_{TA} is the coordinate representing the geographical region controlled by TA, and TS''' is the current timestamp of TA.

Reg_{TA} is used for the handover process when C_v crosses to another geographical region controlled by another trusted authority (e.g., different states, districts, or cities). This process is explained later in the handover protocol section.

DMV, once the message is received from TA, forwards it to the participating vehicle. Finally, C_v verifies the validity of TS''', then decrypts the received message using S_{r1}, and stores the decrypted values into its tamper-proof device.

It is important to note that the DMV only sends 5G_ID_{Cv} to the TA. This means that the relation between C_v and 5G_ID_{Cv} is kept only at the DMV. This will offer the feature of role separation, and consequently, more protection for the real identity of the participating vehicle, since 5G_ID_{Cv} is not a fixed value changeable during the next inspection/registration event.

4.3.3. Official Vehicle Registration Protocol. Figure 3 illustrates both Participation Vehicles Registration and Official Vehicle Registration protocols, but the protocols are executed independently in different time.

The official vehicles are also registered for this service to ensure that only authentic official vehicles will receive the notification of a traffic accident video (see Figure 3). The official designated vehicle generates a random symmetric key $S_{r2} \in Z^{*}{}_{q}$ and sends $\{\text{DV}_i, \text{5G\_ID}_{\text{DV}i}, \text{PKE}(\text{PK}_{\text{TA}}, S_{r2})\}$ to the Law Enforcement Agency (LEA), where DV_i is the unique identification of the official designated vehicle, $\text{5G\_ID}_{\text{DV}i}$ is the 5G identification corresponding to DV_i, and PK_{TA} is the public key of the trusted authority (TA) of the region which C_v and DV_i are part of.

Once the message is received, LEA verifies physically the correctness of DV_i, gets its attribute(s), $\text{Attribute}_{\text{DV}i}$ (e.g., "police vehicle," "ambulance," "traffic authority," or "traffic law enforcement"), and generates the message $M3 = \{\text{5G\_ID}_{\text{DV}i}, \text{TS2}', \text{Attribute}_{\text{DV}i}, \text{PKE}(\text{PK}_{\text{TA}}, S_{r2})\}$ and $\sigma_{M3} = \text{Sign}(\text{SK}_{\text{LEA}}, M3)$, where $\text{TS2}'$ is the current timestamp of LEA, SK_{LEA} is the private key of LEA, and $\text{Sign}(x, y)$ is a digital signing of a message y using a private key x. Upon generating the messages, LEA sends $M3$ and σ_{M3} to TA.

After receiving the message, TA verifies the freshness of the message by checking the fulfillment of $(\text{TS2}''-\text{TS2}') \leq \text{DTS}$, where TS'' is the current timestamp of TA and ΔTS is the timestamp expiration threshold. Only if the message is fresh, the TA verifies the authenticity of the received signature σ_{M3} as follows: $\text{Verify}(\text{PK}_{\text{LEA}}, M3, \sigma_{M3})$. After signature verification, TA obtains S_{r2} by executing $\text{PKD}(\text{SK}_{\text{TA}}, \text{PKE}(\text{PK}_{\text{TA}}, S_{r2}))$ and then generates the Attribute Based Encryption Private Key for DV_i as follows: $\text{SK}_{\text{ABE(TA,DV}i)} = \text{ABE.Delegate}(\text{MK}_{\text{TA}}, \text{Attribute}_{\text{DV}i})$. TA also generates a certificate $\text{Cert}_{\text{TA,5G\_IDDV}i}$ for DV_i based on $\text{5G\_ID}_{\text{DV}i}$ and includes it into a message $M4 = \{T2''', \text{SEnc}(S_{r2}, \text{Cert}_{\text{TA,5G\_IDDV}i}, \text{SK}_{\text{ABE(DV}i)}, T2''', \text{IP}_{\text{Cloud(TA)}})\}$, to finally send it to LEA. LEA receives $M4$ and forwards it to DV_i.

Upon receiving $M4$, DV_i verifies the freshness of the message using ΔTS and decrypts $M4$ by executing $\text{SDec}(S_{r2}, M4)$. Once decrypting $M4$, DV_i compares the decrypted $T2'''$ with the $T2'''$ value received in plaintext to double verify the authenticity and freshness of the message. Finally, DV_i stores the decrypted values into its tamper-proof device.

Now, once registered with TA and LEA, it is time to execute the registration with the Cloud Platform. For this, DV_i sends an registration request message to Cloud_{TA}. Once receiving the request, the Cloud Platform generates a random nonce $N1$ and transmits it to DV_i. Upon receiving $N1$, DV_i generates a random symmetric key S_{r3} and a random nonce $N2$, calculates $M5 = \text{PKE}(\text{PK}_{\text{CloudTA}}, S_{r3})$ and $M6 = \text{SEnc}(S_{r3}, (N1, N2, \text{Cert}_{\text{TA,5G\_IDDV}i}))$, and sends $\{M5, M6\}$ to Cloud_{TA}. The Cloud Platform then obtains S_{r3} by executing $\text{PKD}(\text{SK}_{\text{CloudTA}}, M5)$ and uses such value to obtain $\{N1', N2', \text{Cert}_{\text{TA,5G\_IDDV}i}\} = \text{SDec}(S_{r3}, M6)$. Once with $N1'$, Cloud_{TA} verifies the freshness of the message comparing the decrypted nonce $N1'$ with the one generated previously, $N1$, only if those values matching DV_i are registered to the Cloud Platform. Closing the registration process, Cloud_{TA} registers $\text{Cert}_{\text{TA,5G\_IDDV}i}$ in its database and sends the decrypted $N2'$ to DV_i to confirm its registration. Finally, DV_i verifies the confirmation message by comparing the received $N2'$ with the previously generated $N2$.

It is important to clarify that the communication between DV_i and Cloud_{TA} uses random nonces to validate the freshness of messages instead of timestamps. This is because it is hard to maintain the clock of DV_i and Cloud_{TA} synchronized. Timestamps are only used among LEA, DMV, and TA since they are trusted entities which can coordinate a reliable clock synchronization.

4.3.4. Handover Protocol. The proposed scheme solves the limitation of Eiza-Ni-Shi Scheme regarding the lack of contemplation of different regional areas that are under the management of different trusted authorities. The proposed scheme contributes with a novel handover protocol executed when a participating vehicle C_v goes to a different regional area with another trusted authority.

In Participating Vehicle Registration Protocol, C_v received Reg_{TA} which contains the coordinate of the geographical region controlled by TA. Such value is used to verify when handover is required. For this, C_v checks periodically its GPS coordinate with Reg_{TA}; when $\text{Coordinate}_{Cv} \notin \text{Reg}_{\text{TA}}$, it initiates the handover protocol composed of the following steps (see Figure 4).

First, C_v sends a handover request to TA. The TA then generates a random nonce $N3$ and sends it to C_v. Upon receiving the random nonce, C_v generates its own random nonce $N4$ and a random symmetric key S_{r4} and calculates $M7 = \{\text{PKE}(\text{PK}_{\text{TA}}, S_{r4}), \text{SEnc}(S_{r4}, (N3, N4, \text{5G\_ID}_{Cv}, \text{Coordinate}_{Cv}))\}$ and $\sigma_{M7} = \text{Sign}(\text{SK}_{\text{5G\_IDC}vj}, M7)$. Once calculating such values, C_v sends $(M7, \sigma_{M7}, \text{PCert}_{\text{TA,5G\_IDC}vj})$ to its trusted authority (TA), where $\text{PCert}_{\text{TA,5G\_IDC}vj}$ is the first not used pseudo-certificate valid at current time.

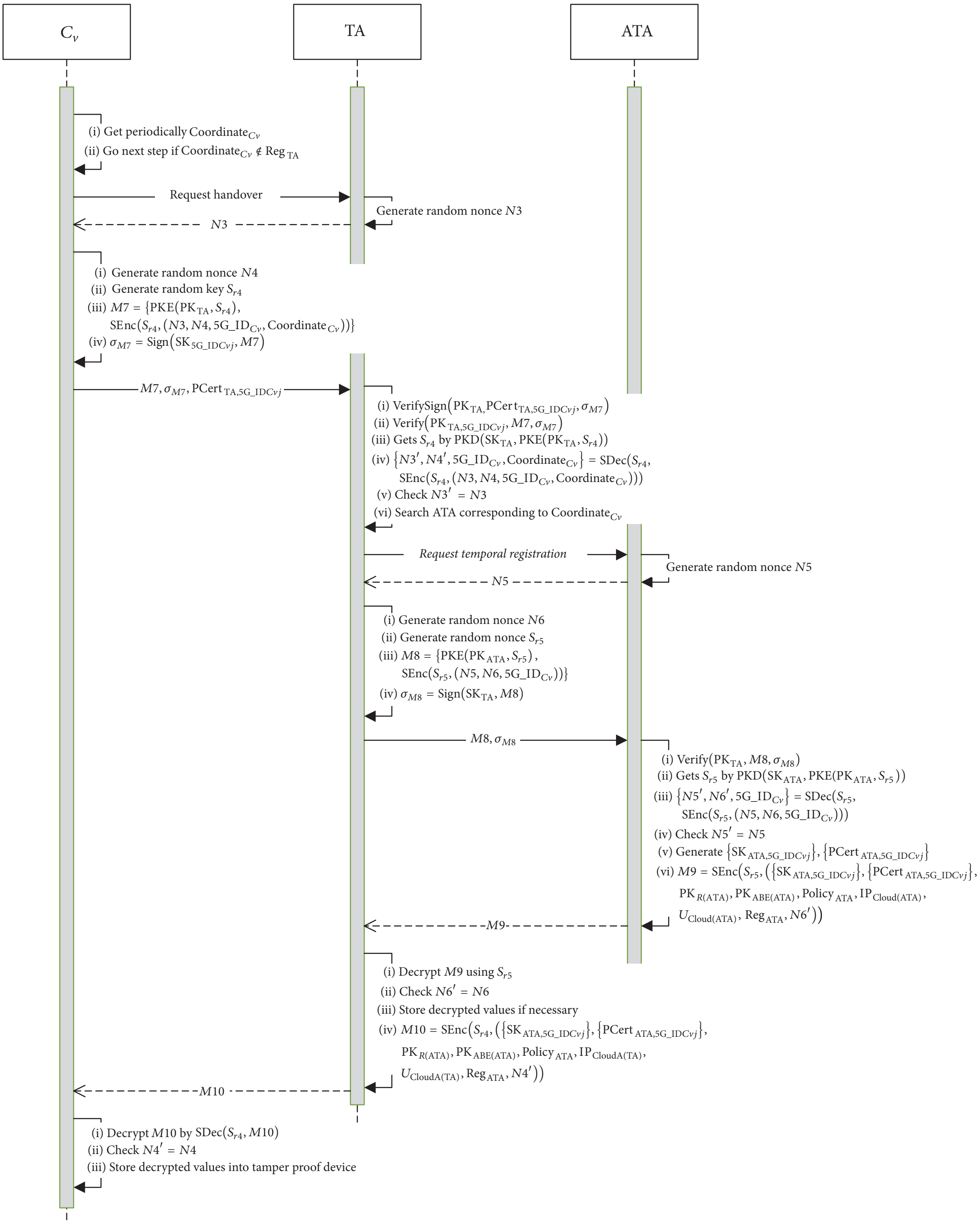

C_v
TA
ATA
(i) Get periodically Coordinate$_{Cv}$
(ii) Go next step if Coordinate$_{Cv}$ ∉ Reg$_{\text{TA}}$
Request handover
Generate random nonce $N3$
$N3$
(i) Generate random nonce $N4$
(ii) Generate random key S_{r4}
(iii) $M7 = \{\text{PKE}(\text{PK}_{\text{TA}}, S_{r4}), \text{SEnc}(S_{r4}, (N3, N4, \text{5G\_ID}_{Cv}, \text{Coordinate}_{Cv}))\}$
(iv) $\sigma_{M7} = \text{Sign}(\text{SK}_{\text{5G\_IDC}vj}, M7)$
$M7, \sigma_{M7}, \text{PCert}_{\text{TA,5G\_IDC}vj}$
(i) $\text{VerifySign}(\text{PK}_{\text{TA}}, \text{PCert}_{\text{TA,5G\_IDC}vj}, \sigma_{M7})$
(ii) $\text{Verify}(\text{PK}_{\text{TA,5G\_IDC}vj}, M7, \sigma_{M7})$
(iii) Gets S_{r4} by $\text{PKD}(\text{SK}_{\text{TA}}, \text{PKE}(\text{PK}_{\text{TA}}, S_{r4}))$
(iv) $\{N3', N4', \text{5G\_ID}_{Cv}, \text{Coordinate}_{Cv}\} = \text{SDec}(S_{r4}, \text{SEnc}(S_{r4}, (N3, N4, \text{5G\_ID}_{Cv}, \text{Coordinate}_{Cv})))$
(v) Check $N3' = N3$
(vi) Search ATA corresponding to Coordinate$_{Cv}$
Request temporal registration
Generate random nonce $N5$
$N5$
(i) Generate random nonce $N6$
(ii) Generate random nonce S_{r5}
(iii) $M8 = \{\text{PKE}(\text{PK}_{\text{ATA}}, S_{r5}), \text{SEnc}(S_{r5}, (N5, N6, \text{5G\_ID}_{Cv}))\}$
(iv) $\sigma_{M8} = \text{Sign}(\text{SK}_{\text{TA}}, M8)$
$M8, \sigma_{M8}$
(i) $\text{Verify}(\text{PK}_{\text{TA}}, M8, \sigma_{M8})$
(ii) Gets S_{r5} by $\text{PKD}(\text{SK}_{\text{ATA}}, \text{PKE}(\text{PK}_{\text{ATA}}, S_{r5}))$
(iii) $\{N5', N6', \text{5G\_ID}_{Cv}\} = \text{SDec}(S_{r5}, \text{SEnc}(S_{r5}, (N5, N6, \text{5G\_ID}_{Cv})))$
(iv) Check $N5' = N5$
(v) Generate $\{\text{SK}_{\text{ATA,5G\_IDC}vj}\}, \{\text{PCert}_{\text{ATA,5G\_IDC}vj}\}$
(vi) $M9 = \text{SEnc}(S_{r5}, (\{\text{SK}_{\text{ATA,5G\_IDC}vj}\}, \{\text{PCert}_{\text{ATA,5G\_IDC}vj}\}, \text{PK}_{R(\text{ATA})}, \text{PK}_{\text{ABE(ATA)}}, \text{Policy}_{\text{ATA}}, \text{IP}_{\text{Cloud(ATA)}}, U_{\text{Cloud(ATA)}}, \text{Reg}_{\text{ATA}}, N6'))$
$M9$
(i) Decrypt $M9$ using S_{r5}
(ii) Check $N6' = N6$
(iii) Store decrypted values if necessary
(iv) $M10 = \text{SEnc}(S_{r4}, (\{\text{SK}_{\text{ATA,5G\_IDC}vj}\}, \{\text{PCert}_{\text{ATA,5G\_IDC}vj}\}, \text{PK}_{R(\text{ATA})}, \text{PK}_{\text{ABE(ATA)}}, \text{Policy}_{\text{ATA}}, \text{IP}_{\text{CloudA(TA)}}, U_{\text{CloudA(TA)}}, \text{Reg}_{\text{ATA}}, N4'))$
$M10$
(i) Decrypt $M10$ by $\text{SDec}(S_{r4}, M10)$
(ii) Check $N4' = N4$
(iii) Store decrypted values into tamper proof device

Figure 4: Proposed handover protocol.

Once receiving the message, TA verifies the authenticity of σ_{M7} and origin of $\text{PCert}_{\text{TA,5G\_IDC}vj}$ by executing $\text{VerifySign}(\text{PK}_{\text{TA}}, \text{PCert}_{\text{TA,5G\_IDC}vj}, \sigma_{M7})$. TA also verifies if σ_{M7} corresponds to the digital signature of $M7$ by performing $\text{Verify}(\text{PK}_{\text{TA,5G\_IDC}vj}, M7, \sigma_{M7})$. Once the authenticity of messages is verified, TA gets S_{r4} by $\text{PKD}(\text{SK}_{\text{TA}}, \text{PKE}(\text{PK}_{\text{TA}}, S_{r4}))$ and uses it to obtain $\{N3', N4', \text{5G\_ID}_{Cv}, \text{Coordinate}_{Cv}\} = \text{SDec}(S_{r4}, \text{SEnc}(S_{r4}, (N3, N4, \text{5G\_ID}_{Cv}, \text{Coordinate}_{Cv})))$. Upon decrypting the data, TA verifies the freshness of the message by comparing the decrypted $N3'$ with the previously generated $N3$. The nonce comparison allows TA to eliminate all possibilities of replay attacks from adversaries. Once the validity of handover request is verified, TA searches the away trusted authority (ATA) that controls the region where C_v currently is located.

Once the adequate ATA is detected, TA mediates the registration of C_v in ATA. For this, TA requests a temporal registration of C_v to ATA. Upon receiving the request, ATA generates a random nonce $N5$ and sends it to TA. Once the connection with ATA is realized, TA generates a random nonce $N6$ and a random symmetric key S_{r5} and calculates $M8 = \{\text{PKE}(\text{PK}_{\text{ATA}}, S_{r5}), \text{SEnc}(S_{r5}, (N5, N6, \text{5G\_ID}_{Cv}))\}$ and $\sigma_{M8} = \text{Sign}(\text{SK}_{\text{TA}}, M8)$. Once the messages are calculated, TA sends $(M8, \sigma_{M8})$ to ATA.

Once receiving the message, ATA verifies the authenticity of the received signature σ_{M8} as follows: $\text{Verify}(\text{PK}_{\text{TA}}, M8, \sigma_{M8})$. Upon signature verification, ATA obtains S_{r5} by executing $\text{PKD}(\text{SK}_{\text{ATA}}, \text{PKE}(\text{PK}_{\text{ATA}}, S_{r5}))$ and uses such value to get $\{N5', N6', \text{5G\_ID}_{Cv}\} = \text{SDec}(S_{r5}, \text{SEnc}(S_{r5}, (N5, N6, \text{5G\_ID}_{Cv})))$. Later, ATA verifies the freshness of the message comparing the decrypted nonce $N5'$ with the previously generated $N5$. Only if those values match, ATA proceeds to respond to the registration request. Closing the temporal registration process, ATA generates the set of private keys $\{\text{SK}_{\text{ATA,5G\_ID}Cvj}\}$ and a set of pseudonymous certificates $\{\text{PCert}_{\text{ATA,5G\_ID}Cvj}\}$ corresponding to 5G_ID_{Cv} of C_v. After that, ATA returns the message $M9 = \text{SEnc}(S_{r5}, (\{\text{SK}_{\text{ATA,5G\_ID}Cvj}\}, \{\text{PCert}_{\text{ATA,5G\_ID}Cvj}\}, \text{PK}_{R(\text{ATA})}, \text{PK}_{\text{ABE(ATA)}}, \text{Policy}_{\text{ATA}}, \text{IP}_{\text{Cloud(ATA)}}, U_{\text{Cloud(ATA)}}, \text{Reg}_{\text{ATA}}, N6'))$ to TA, where $\text{PK}_{R(\text{ATA})}$ is the public key of ATA for Public Key Encryption with Keyword Search, $\text{PK}_{\text{ABE(ATA)}}$ is the public key of ATA for the Attributed Based Encryption, $\text{Policy}_{\text{ATA}}$ is the access policy of traffic accident videos uploaded by C_v (e.g., $\text{Policy}_{\text{ATA}}$ = {"police vehicle" OR "ambulance" OR "traffic law enforcement" OR "traffic authority"}), $\text{IP}_{\text{Cloud(ATA)}}$ is the IP address of the Cloud Platform of ATA, $U_{\text{Cloud(ATA)}} \in Z^*_q$ is the a tag preagreed upon between ATA and the Cloud Platform of ATA ($\text{Cloud}_{\text{ATA}}$), and Reg_{ATA} is the coordinate representing the geographical region controlled by ATA.

Upon receiving the response from ATA, TA decrypts $M9$ using its random key S_{r5}. Once decrypting $M9$, TA verifies the authenticity of $M9$ by comparing $N6'$ with its own $N6$. This comparison allows TA to be sure that $M9$ came from the valid ATA. After verification, TA stores the decrypted values for historical data of C_v (only if required) and generates a new message $M10 = \text{SEnc}(S_{r4}, (\{\text{SK}_{\text{ATA,5G\_ID}Cvj}\}, \{\text{PCert}_{\text{ATA,5G\_ID}Cvk}\}, \text{PK}_{R(\text{ATA})}, \text{PK}_{\text{ABE(ATA)}}, \text{Policy}_{\text{ATA}}, \text{IP}_{\text{Cloud(ATA)}}, U_{\text{Cloud(ATA)}}, \text{Reg}_{\text{ATA}}, N4'))$ and sends it to C_v.

Upon receiving the message, C_v decrypts $M10$ and verifies that the message came from the authentic TA freshly by comparing $N4'$ with $N4$. After verification C_v stores the decrypted values to its tamper-proof device.

Note. Since the trusted authorities are in different regional areas and as it is hard to have clock synchronization, handshake using random nonces is used instead of timestamps to avoid replay attacks.

4.3.5. Video Transmission Protocol. When an accident occurs, C_v obtains the recorded video file through its cameras and initiates the video transmission protocol, which is composed of the following steps (see Figure 5).

First, C_v generates a random symmetric key S_{r6} and uses it to encrypt the video file TV_r and its current GPS coordinate $\textit{Coordinate}_{Cv}$ as follows: $\text{ETV}_r = \text{SEnc}(S_{r6}, (\text{TV}_r, \text{Coordinate}_{Cv}))$. Then, C_v generates the keywords related to the accident kw and encrypts it using the Public Key Encryption with Keyword Search function as $\text{Ekw} = \text{PEKS}(\text{PK}_{R(\text{TA})}, \text{kw})$ and calculates $\text{ES}_{r6} = \text{ABE.Enc}(\text{PK}_{\text{ABE(TA)}}, S_{r6}, \text{Policy})$. Additionally, C_v encrypts S_{r6} using the Attribute Based Encryption function using $\text{PK}_{\text{ABE(TA)}}$ and *Policy* and creates a digital signature $\sigma_{\text{5G\_ID}Cvj}$ of generated messages using its current private key $\text{SK}_{\text{TA,5G\_ID}Cvj}$. Finally, C_v clusters the generated messages into $M11 = \{h(U_{\text{Cloud(TA)}}), \text{ETV}_r, \text{Ekw}, \text{ES}_{r6}, \sigma_{\text{5G\_ID}Cvj}, \text{PCert}_{\text{TA,5G\_ID}Cvj}\}$ and sends it to Cloud_{TA} over the 5G enabled vehicular network.

Upon receiving $M11$, Cloud_{TA} checks if $\text{PCert}_{\text{TA,5G\_ID}Cvj}$ is in the Pseudo-Certificate Revocation List, $\text{PCRL}_{\text{Cloud(TA)}}$, or in the Used Pseudo-Certificate List, $\text{UPCL}_{\text{Cloud(TA)}}$, which is the list of the already used pseudo-certificates. It is important to remember that a pseudo-certificate is usable only once. If such pseudo-certificate is in $\text{PCRL}_{\text{Cloud(TA)}}$ or $\text{UPCL}_{\text{Cloud(TA)}}$, the received $M11$ is discarded; otherwise, Cloud_{TA} verifies the authenticity of the message by executing $\text{VerifySign}(\text{PK}_{\text{TA}}, \text{PCert}_{\text{TA,5G\_ID}Cvj}, \sigma_{\text{5G\_ID}Cvj})$. If the certificate is proved to be valid, Cloud_{TA} stores such message and notifies the nearest designated vehicle DV_i about the accident sending $M11$. We assume that the location information of the official vehicles is updated periodically in the cloud. The location of official vehicles is protected since it is transmitted using the public key of Cloud_{TA} $\text{PK}_{\text{CloudTA}}$.

Once an official vehicle DV_i receives the notification, it verifies the received pseudonymous certificate $\text{PCert}_{\text{TA,5G\_ID}Cvj}$ by executing $\text{VerifySign}(\text{PK}_{\text{TA}}, \text{PCert}_{\text{TA,5G\_ID}Cvj}, \sigma_{\text{5G\_ID}Cvj})$. If the certificate is proved to be valid, DV_i extracts the public key $\text{PK}_{\text{TA,5G\_ID}Cvj}$ of the sender from the certificate $\text{PCert}_{\text{TA,5G\_ID}Cvj}$. Upon certificate validation, DV_i verifies the received signature $\sigma_{\text{5G\_ID}Cvj}$ by executing $\text{Verify}(\text{PK}_{\text{TA,5G\_ID}Cvj}, (h(U_{\text{Cloud(TA)}}), \text{ETV}_r, \text{Ekw}, \text{ES}_{r6}), \sigma_{\text{5G\_ID}Cvj})$ and obtains the S_{r6} using its Attributed Based Encryption private key $\text{SK}_{\text{ABE(TA,DV}i)}$ as follows: $S_{r6} = \text{ABE.Dec}(\text{ES}_{r6}, \text{SK}_{\text{ABE(TA,DV}i)})$. Finally, DV_i gets the decrypted video and the last coordinate of C_v by executing $(\text{TV}_r, \text{Coordinate}_{Cv}) = \text{SDec}(S_{r6}, \text{ETV}_r)$. Now, the official vehicles are able to go to the location of the accident using Coordinate_{Cv} and they can check the video of the accident while going to the location.

4.3.6. Video Search Protocol. Once the video transmission protocol is done and the video is uploaded to the Cloud Platform, it can be retrieved by LEA whenever it is needed. The video search protocol is executed as follows (see Figure 5).

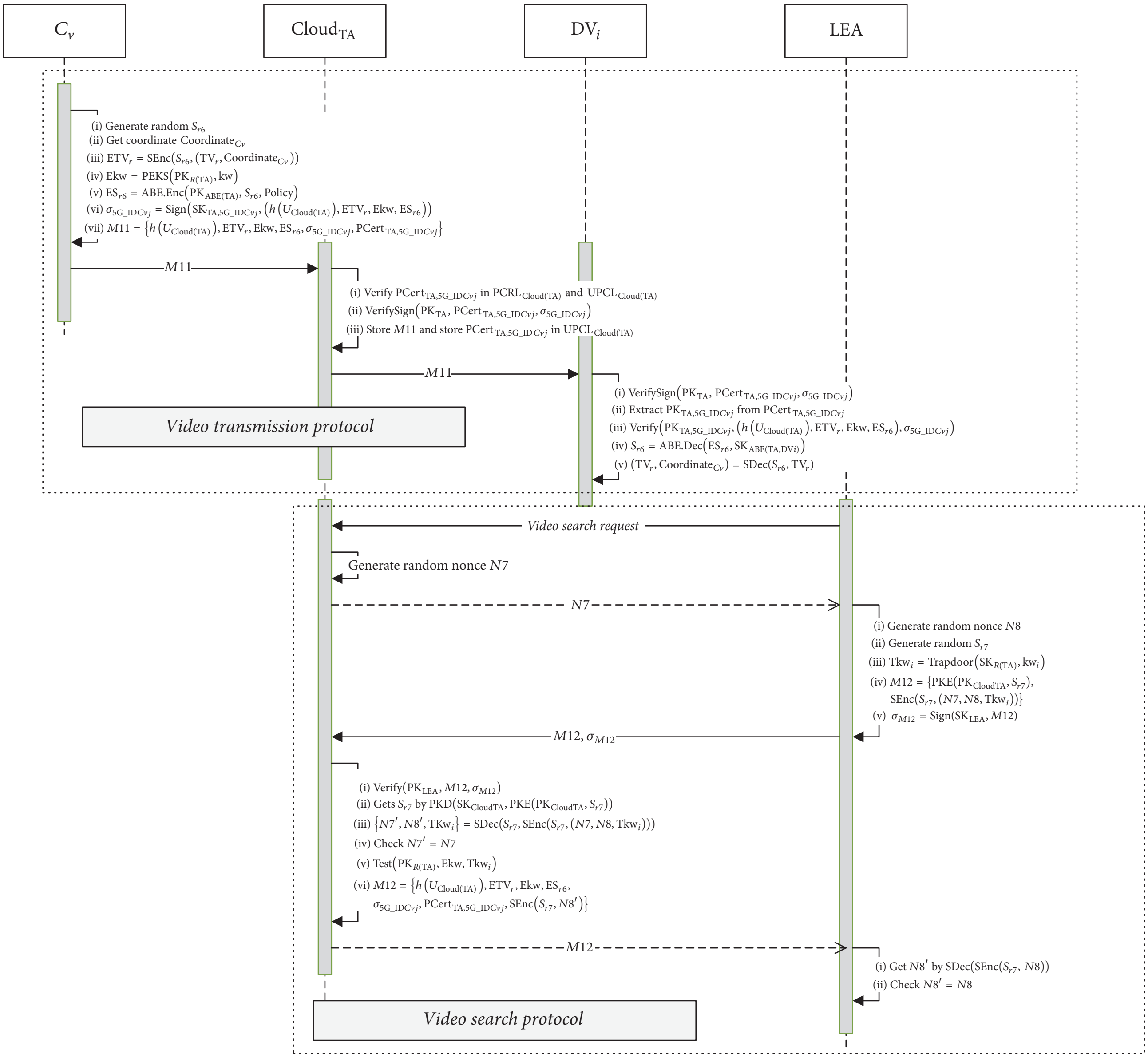

C_v
Cloud_{TA}
DV_i
LEA
(i) Generate random S_{r6}
(ii) Get coordinate Coordinate_{Cv}
(iii) $\text{ETV}_r = \text{SEnc}(S_{r6}, (\text{TV}_r, \text{Coordinate}_{Cv}))$
(iv) $\text{Ekw} = \text{PEKS}(\text{PK}_{R(\text{TA})}, \text{kw})$
(v) $\text{ES}_{r6} = \text{ABE.Enc}(\text{PK}_{\text{ABE(TA)}}, S_{r6}, \text{Policy})$
(vi) $\sigma_{5\text{G\_ID}Cvj} = \text{Sign}(\text{SK}_{\text{TA,5G\_ID}Cvj}, (h(U_{\text{Cloud(TA)}}), \text{ETV}_r, \text{Ekw}, \text{ES}_{r6}))$
(vii) $M11 = \{h(U_{\text{Cloud(TA)}}), \text{ETV}_r, \text{Ekw}, \text{ES}_{r6}, \sigma_{5\text{G\_ID}Cvj}, \text{PCert}_{\text{TA,5G\_ID}Cvj}\}$
$M11$
(i) Verify $\text{PCert}_{\text{TA,5G\_ID}Cvj}$ in $\text{PCRL}_{\text{Cloud(TA)}}$ and $\text{UPCL}_{\text{Cloud(TA)}}$
(ii) $\text{VerifySign}(\text{PK}_{\text{TA}}, \text{PCert}_{\text{TA,5G\_ID}Cvj}, \sigma_{5\text{G\_ID}Cvj})$
(iii) Store $M11$ and store $\text{PCert}_{\text{TA,5G\_ID}Cvj}$ in $\text{UPCL}_{\text{Cloud(TA)}}$
$M11$
(i) $\text{VerifySign}(\text{PK}_{\text{TA}}, \text{PCert}_{\text{TA,5G\_ID}Cvj}, \sigma_{5\text{G\_ID}Cvj})$
(ii) Extract $\text{PK}_{\text{TA,5G\_ID}Cvj}$ from $\text{PCert}_{\text{TA,5G\_ID}Cvj}$
(iii) $\text{Verify}(\text{PK}_{\text{TA,5G\_ID}Cvj}, (h(U_{\text{Cloud(TA)}}), \text{ETV}_r, \text{Ekw}, \text{ES}_{r6}), \sigma_{5\text{G\_ID}Cvj})$
(iv) $S_{r6} = \text{ABE.Dec}(\text{ES}_{r6}, \text{SK}_{\text{ABE(TA,DV}i)})$
(v) $(\text{TV}_r, \text{Coordinate}_{Cv}) = \text{SDec}(S_{r6}, \text{TV}_r)$
Video transmission protocol
Video search request
Generate random nonce $N7$
$N7$
(i) Generate random nonce $N8$
(ii) Generate random S_{r7}
(iii) $\text{Tkw}_i = \text{Trapdoor}(\text{SK}_{R(\text{TA})}, \text{kw}_i)$
(iv) $M12 = \{\text{PKE}(\text{PK}_{\text{CloudTA}}, S_{r7}),$
$\text{SEnc}(S_{r7}, (N7, N8, \text{Tkw}_i))\}$
(v) $\sigma_{M12} = \text{Sign}(\text{SK}_{\text{LEA}}, M12)$
$M12, \sigma_{M12}$
(i) $\text{Verify}(\text{PK}_{\text{LEA}}, M12, \sigma_{M12})$
(ii) Gets S_{r7} by $\text{PKD}(\text{SK}_{\text{CloudTA}}, \text{PKE}(\text{PK}_{\text{CloudTA}}, S_{r7}))$
(iii) $\{N7', N8', \text{TKw}_i\} = \text{SDec}(S_{r7}, \text{SEnc}(S_{r7}, (N7, N8, \text{Tkw}_i)))$
(iv) Check $N7' = N7$
(v) $\text{Test}(\text{PK}_{R(\text{TA})}, \text{Ekw}, \text{Tkw}_i)$
(vi) $M12 = \{h(U_{\text{Cloud(TA)}}), \text{ETV}_r, \text{Ekw}, \text{ES}_{r6},$
$\sigma_{5\text{G\_ID}Cvj}, \text{PCert}_{\text{TA,5G\_ID}Cvj}, \text{SEnc}(S_{r7}, N8')\}$
$M12$
(i) Get $N8'$ by $\text{SDec}(\text{SEnc}(S_{r7}, N8))$
(ii) Check $N8' = N8$
Video search protocol

FIGURE 5: Video transmission and video search protocols.

First, LEA initiates a video search request to Cloud_{TA}. Then, Cloud_{TA} generates a random nonce $N7$ and sends it to LEA. Once receiving the response of Cloud_{TA}, LEA generates another random nonce $N8$ and a random symmetric key S_{r7} and then generates the searchable trapdoor token as follows: $\text{Tkw}_i = \text{Trapdoor}(\text{SK}_{R(\text{TA})}, \text{kw}_i)$, where kw_i is a keyword (e.g., location, date, or "any video") related to the video. Upon generation of the search token, LEA generates a message $M12 = \{\text{PKE}(\text{PK}_{\text{CloudTA}}, S_{r7}), \text{SEnc}(S_{r7}, (N7, N8, \text{Tkw}_i))\}$ and its digital signature $\sigma_{M12} = \text{Sign}(\text{SK}_{\text{LEA}}, M12)$ and sends them to the Cloud_{TA}.

On the other side, Cloud_{TA} verifies the validity of the digital signature σ_{M12} by performing $\text{Verify}(\text{PK}_{\text{LEA}}, M12, \sigma_{M12})$ to be sure that the search request comes from the authentic LEA. Once validating the authenticity of the message, the Cloud Platform extracts S_{r7} by $\text{PKD}(\text{SK}_{\text{CloudTA}}, \text{PKE}(\text{PK}_{\text{CloudTA}}, S_{r7}))$ and uses it to get $\{N7', N8', \text{Tkw}_i\} = \text{SDec}(S_{r7}, \text{SEnc}(S_{t7}, (N7, N8, \text{Tkw}_i)))$. Once obtaining the data, Cloud_{TA} verifies the freshness of the message by comparing the decrypted nonce $N7'$ with the previously generated $N7$. If those values match, Cloud_{TA} authorizes Tkw_i search process over the ciphertext at the cloud and executes $\text{Test}(\text{PK}_{R(\text{TA})}, \text{Ekw}, \text{Tkw}_i)$. Once the video is founded, a new message $M12 = \{h(U_{\text{Cloud(TA)}}), \text{ETV}_r, \text{Ekw}, \text{ES}_{r6}, \sigma_{5\text{G\_ID}Cvj}, \text{PCert}_{\text{TA,5G\_ID}Cvj}, \text{SEnc}(S_{r7}, N8)\}$ is generated and it is sent to the LEA.

Upon receiving $M12$, LEA extracts $N8'$ by executing $\text{SDec}(\text{SEnc}(S_{r7}, N8'))$ and compares it with the previously generated $N8$ to validate the authenticity and freshness of the message. The comparison of random nonces allows LEA to verify the freshness since the received nonce corresponds

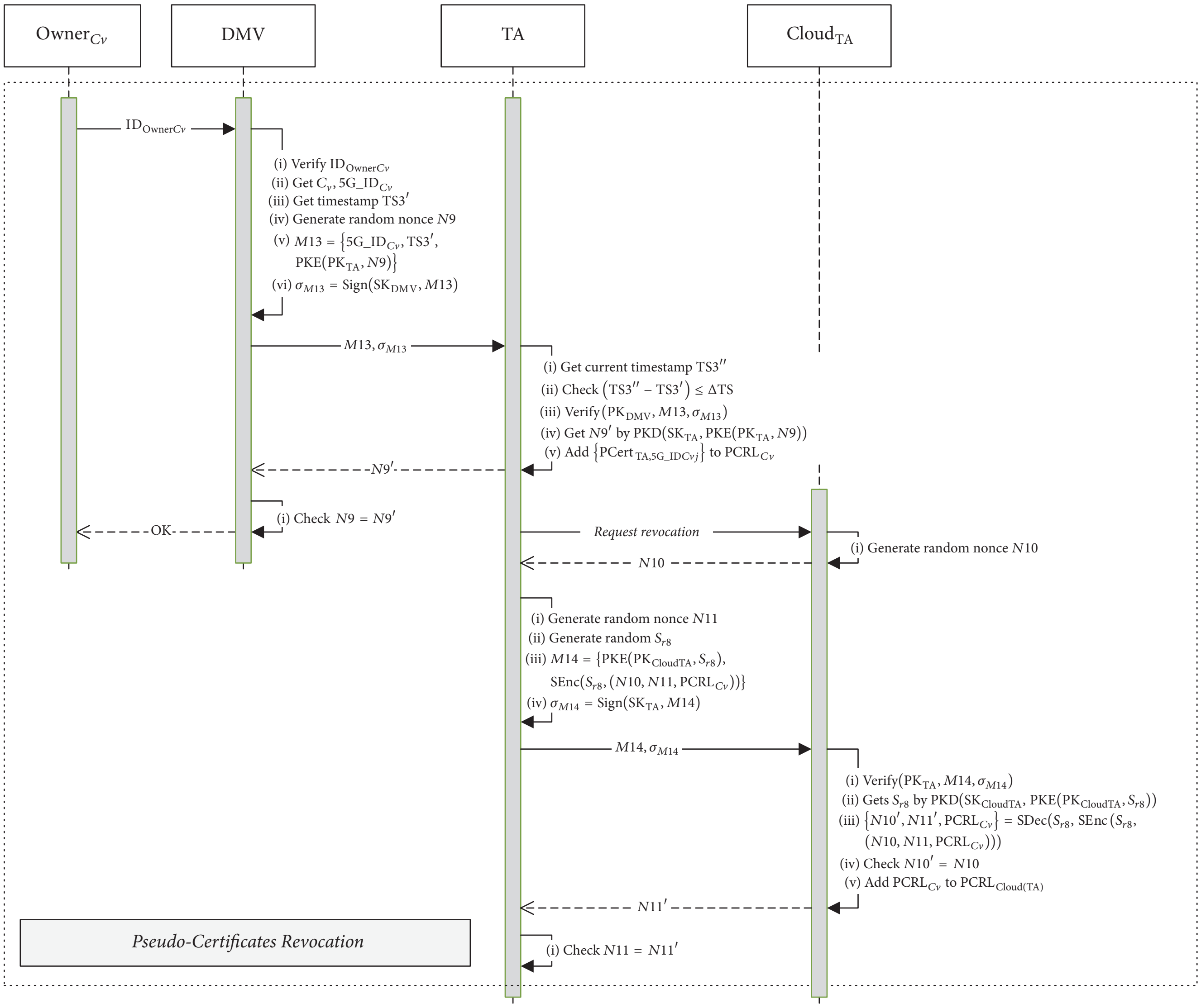

Owner_{Cv}
DMV
TA
Cloud_{TA}
$\text{ID}_{\text{Owner}Cv}$
(i) Verify $\text{ID}_{\text{Owner}Cv}$
(ii) Get C_v, 5G_ID_{Cv}
(iii) Get timestamp $\text{TS3}'$
(iv) Generate random nonce $N9$
(v) $M13 = \{\text{5G\_ID}_{Cv}, \text{TS3}', \text{PKE}(\text{PK}_{\text{TA}}, N9)\}$
(vi) $\sigma_{M13} = \text{Sign}(\text{SK}_{\text{DMV}}, M13)$
$M13, \sigma_{M13}$
(i) Get current timestamp $\text{TS3}''$
(ii) Check $(\text{TS3}'' - \text{TS3}') \leq \Delta\text{TS}$
(iii) Verify$(\text{PK}_{\text{DMV}}, M13, \sigma_{M13})$
(iv) Get $N9'$ by $\text{PKD}(\text{SK}_{\text{TA}}, \text{PKE}(\text{PK}_{\text{TA}}, N9))$
(v) Add $\{\text{PCert}_{\text{TA,5G\_ID}Cvj}\}$ to PCRL_{Cv}
$N9'$
(i) Check $N9 = N9'$
OK
Request revocation
(i) Generate random nonce $N10$
$N10$
(i) Generate random nonce $N11$
(ii) Generate random S_{r8}
(iii) $M14 = \{\text{PKE}(\text{PK}_{\text{CloudTA}}, S_{r8}), \text{SEnc}(S_{r8}, (N10, N11, \text{PCRL}_{Cv}))\}$
(iv) $\sigma_{M14} = \text{Sign}(\text{SK}_{\text{TA}}, M14)$
$M14, \sigma_{M14}$
(i) Verify$(\text{PK}_{\text{TA}}, M14, \sigma_{M14})$
(ii) Gets S_{r8} by $\text{PKD}(\text{SK}_{\text{CloudTA}}, \text{PKE}(\text{PK}_{\text{CloudTA}}, S_{r8}))$
(iii) $\{N10', N11', \text{PCRL}_{Cv}\} = \text{SDec}(S_{r8}, \text{SEnc}(S_{r8}, (N10, N11, \text{PCRL}_{Cv})))$
(iv) Check $N10' = N10$
(v) Add PCRL_{Cv} to $\text{PCRL}_{\text{Cloud(TA)}}$
$N11'$
(i) Check $N11 = N11'$
Pseudo-Certificates Revocation

Figure 6: Pseudo-Certificates Revocation Protocol.

to the last one created by itself. The nonce comparison also allows the verification of authenticity of Cloud_{TA} since the sent nonce can only be decrypted by the authentic Cloud_{TA} having the private key $\text{SK}_{\text{CloudTA}}$.

4.3.7. Pseudo-Certificate Revocation. This protocol is executed when a participating vehicle C_v needs to stop its participation in the video reporting services, either because the user expressed his/her willingness to stop the service, because the car was robbed, or because the pseudo-certificates stored in the car have been exposed. This protocol is composed of the following steps (see Figure 6).

First, the owner of the participating vehicle Owner_{Cv} indicates his/her willingness to stop the video reporting services to the DMV by delivering his/her identification $\text{ID}_{\text{Owner}Cv}$ (e.g., driver's license). Once the request is received, the DMV verifies the authenticity of $\text{ID}_{\text{Owner}Cv}$ and gets C_v and 5G_ID_{Cv} corresponding to Owner_{Cv}. Then, the DMV gets its current timestamp $\text{TS3}'$, generates a random nonce $N9$, and calculates $M13 = \{\text{5G\_ID}_{Cv}, \text{TS3}', \text{PKE}(\text{PK}_{\text{TA}}, N9)\}$ and $\sigma_{M13} = \text{Sign}(\text{SK}_{\text{DMV}}, M13)$. Once such values are calculated, DMV sends $(M13, \sigma_{M13})$ to the TA. Once the message is received, TA verifies the freshness of the message using its timestamp $\text{TS3}''$ and verifies the authenticity of σ_{M13} by executing $\text{Verify}(\text{PK}_{\text{DMV}}, M13, \sigma_{M13})$. Once the authenticity of the message is verified, TA gets $N9$ by $\text{PKD}(\text{SK}_{\text{TA}}, \text{PKE}(\text{PK}_{\text{TA}}, N9))$ and adds the pseudo-certificates belonging to 5G_ID_{Cv} to C_v's Peudo-Certificate Revocation List, PCRL_{Cv}. Once PCRL_{Cv} is updated, DMV returns the decrypted $N9'$ to DVM. Finally, the DMV verifies the correct execution of the request by comparing the received message with the $N9$ generated by itself and then informs the Owner_{Cv} about the correct execution of the requested process.

On the other hand, the TA executes the Pseudo-Certificates Revocation process with the Cloud Platform. For this, the TA sends a request message to Cloud_{TA}. Cloud_{TA} then generates a random nonce $N10$ and sends it to TA. Upon receiving the random nonce, TA generates its own random nonce $N11$ and a random symmetric key S_{r8} and calculates $M14 = \{\mathrm{PKE}(\mathrm{PK}_{\mathrm{CloudTA}}, S_{r8}), \mathrm{SEnc}(S_{r8}, (N10, N11, \mathrm{PCRL}_{Cv}))\}$ and $\sigma_{M14} = \mathrm{Sign}(\mathrm{SK}_{\mathrm{TA}}, M14)$. Once such values are calculated, TA sends $(M14, \sigma_{M14})$ to its Cloud Platform. Once the message is received, $\mathrm{Cloud}_{\mathrm{TA}}$ verifies the authenticity of the message by executing $\mathrm{Verify}(\mathrm{PK}_{\mathrm{TA}}, M14, \sigma_{M14})$. Once the authenticity of the message is verified, $\mathrm{Cloud}_{\mathrm{TA}}$ gets S_{r8} by $\mathrm{PKD}(\mathrm{SK}_{\mathrm{CloudTA}}, \mathrm{PKE}(\mathrm{PK}_{\mathrm{CloudTA}}, S_{r8}))$ and uses it to obtain $(N10', N11', \mathrm{PCRL}_{Cv}) = \mathrm{SDec}(S_{r4}, \mathrm{SEnc}(S_{r8}, (N10, N11, \mathrm{PCRL}_{Cv})))$. Upon decrypting the data, TA verifies the freshness of the message by comparing the decrypted $N10'$ with the previously generated $N10$. Once the validity of Pseudo-Certificates Revocation request is verified, $\mathrm{Cloud}_{\mathrm{TA}}$ adds PCRL_{Cv} to the Pseudo-Certificates Revocation List of the Cloud Platform, $\mathrm{PCRL}_{\mathrm{Cloud(TA)}}$. Once $\mathrm{PCRL}_{\mathrm{Cloud(TA)}}$ is updated, $\mathrm{Cloud}_{\mathrm{TA}}$ returns the decrypted $N11'$ to TA. Finally, the TA verifies the correct execution of the request by comparing the received message with the $N11$ generated by itself.

Note. The Pseudo-Certificates Revocation Protocol can also be executed by a designated authority (e.g., police officer) when detecting a misbehaving C_v. In this case, the designated authority requests the Pseudo-Certificates Revocation to LEA instead of DMV. The following steps will be the same; the only difference is that the participating entities will be LEA–TA–$\mathrm{Cloud}_{\mathrm{TA}}$ instead of DMV–TA–$\mathrm{Cloud}_{\mathrm{TA}}$.

4.3.8. Interregion Pseudo-Certificate Revocation. This stage is executed after the Pseudo-Certificate Revocation Protocol, only if the participating vehicle C_v has been in another region and received pseudo-certificates from an ATA. TA can know if C_v has been in another region since it was the intermediary executing the handover protocol. This protocol is composed of the following steps (see Figure 7).

First, TA sends a Pseudo-Certificates Revocation request to ATA where C_v has received pseudo-certificates. The ATA then generates a random nonce $N12$ and sends it to TA. Upon receiving the random nonce, TA generates its own random nonce $N13$ and a random symmetric key S_{r9} and calculates $M15 = \{\mathrm{PKE}(\mathrm{PK}_{\mathrm{TA}}, S_{r9}), \mathrm{SEnc}(S_{r9}, (N12, N13, \mathrm{5G\_ID}_{Cv}, \mathrm{PCRL}_{Cv}))\}$, and $\sigma_{M15} = \mathrm{Sign}(\mathrm{SK}_{\mathrm{TA}}, M15)$. Once such values are calculated, TA sends $(M15, \sigma_{M15})$ to ATA. Once the message is received, ATA verifies the authenticity of the message by executing $\mathrm{Verify}(\mathrm{PK}_{\mathrm{TA}}, M15, \sigma_{M15})$. After verification, ATA gets S_{r9} by $\mathrm{PKD}(\mathrm{SK}_{\mathrm{TA}}, \mathrm{PKE}(\mathrm{PK}_{\mathrm{TA}}, S_{r9}))$ and uses it to obtain $\{N12', N13', \mathrm{5G\_ID}_{Cv}, \mathrm{PCRL}_{Cv}\} = \mathrm{SDec}(S_{r9}, \mathrm{SEnc}(S_{r9}, (N12, N13, \mathrm{5G\_ID}_{Cv}, \mathrm{PCRL}_{Cv})))$. Upon decrypting the data, ATA verifies the freshness of the message by comparing the decrypted $N12'$ with the previously generated $N12$. Once the validity of the request is verified, ATA adds the pseudo-certificates belonging to $\mathrm{5G\_ID}_{Cv}$ to C_v's Pseudo-Certificate Revocation List, PCRL_{Cv}.

On the other hand, the ATA also executes the Pseudo-Certificates Revocation process with the Cloud Platform. For this, the ATA sends a request message to $\mathrm{Cloud}_{\mathrm{ATA}}$. $\mathrm{Cloud}_{\mathrm{ATA}}$ then generates a random nonce $N14$ and sends it to ATA. Upon receiving the random nonce, ATA generates its own random nonce $N15$ and a random symmetric key S_{r10} and calculates $M16 = \{\mathrm{PKE}(\mathrm{PK}_{\mathrm{CloudATA}}, S_{r10}), \mathrm{SEnc}(S_{r10}, (N14, N15, \mathrm{PCRL}_{Cv}))\}$, and $\sigma_{M16} = \mathrm{Sign}(\mathrm{SK}_{\mathrm{ATA}}, M16)$. Once such values are calculated, ATA sends $(M16, \sigma_{M16})$ to its Cloud Platform. Once the message is received, $\mathrm{Cloud}_{\mathrm{ATA}}$ verifies the authenticity of the message by executing $\mathrm{Verify}(\mathrm{PK}_{\mathrm{ATA}}, M16, \sigma_{M16})$. Once the authenticity of the message is verified, $\mathrm{Cloud}_{\mathrm{ATA}}$ gets S_{r10} by $\mathrm{PKD}(\mathrm{SK}_{\mathrm{CloudATA}}, \mathrm{PKE}(\mathrm{PK}_{\mathrm{CloudATA}}, S_{r10}))$ and uses it to obtain $(N14', N15', \mathrm{PCRL}_{Cv}) = \mathrm{SDec}(S_{r10}, \mathrm{SEnc}(S_{r10}, (N14, N15, \mathrm{PCRL}_{Cv})))$. Upon decrypting the data, $\mathrm{Cloud}_{\mathrm{ATA}}$ verifies the freshness of the message by comparing the decrypted $N14'$ with the previously generated $N14$. Once the validity of Pseudo-Certificates Revocation request is verified, $\mathrm{Cloud}_{\mathrm{ATA}}$ adds PCRL_{Cv} to the Pseudo-Certificates Revocation List of the Cloud Platform $\mathrm{PCRL}_{\mathrm{Cloud(ATA)}}$. Once $\mathrm{PCRL}_{\mathrm{Cloud(ATA)}}$ is updated, $\mathrm{Cloud}_{\mathrm{ATA}}$ returns the decrypted $N15'$ to ATA. Finally, the ATA verifies the correct execution of the request by comparing the received message with the $N15$ generated by itself.

4.4. Security Analysis of the Proposed Solution. This section analyzes the proposed scheme in terms of security. It shows how the enhanced solution is secure against different attacks and it is superior to the previous work (see Table 1).

Authentication and Nonrepudiation. The proposed solution provides authentication and nonrepudiation of videos by using the fundaments of public key cryptography. The Cloud Platform can be sure that the video is uploaded by an authentic participant vehicle since C_v delivers its pseudonymous certificate $\mathrm{PCert}_{\mathrm{TA,5G\_ID}Cvj}$. Such certificate can be validated by using the public key of the trusted authority which issued such certificate.

Conditional Anonymity and Privacy. As well as in the previous work, the proposed solution provides conditional anonymity and privacy by using the pseudonymous authentication technique. Since the video is authenticated with the pseudonymous certificate, even if the Cloud Platform is compromised, the adversary U_a will not be able to know the real identity of the participating vehicle. Additionally, since each pseudonymous certificate is usable once and has an expiration time, it will be infeasible for U_a to correlate C_v with $\mathrm{PCert}_{\mathrm{TA,5G\_ID}Cvj}$.

DMV Impersonation Attack. DMV impersonation attack is avoided using the principles of public key cryptography. The participant vehicle registration request message $M1$ is accompanied with its digital signature σ_{M1} signed by the private key of DMV. The TA can verify the origin of the message since it can verify the authenticity of σ_{M1} using the public key of DMV $\mathrm{PK}_{\mathrm{DMV}}$.

Forged Video Upload. Thanks to the protection against the DMV impersonation attack, the adversary U_a cannot obtain

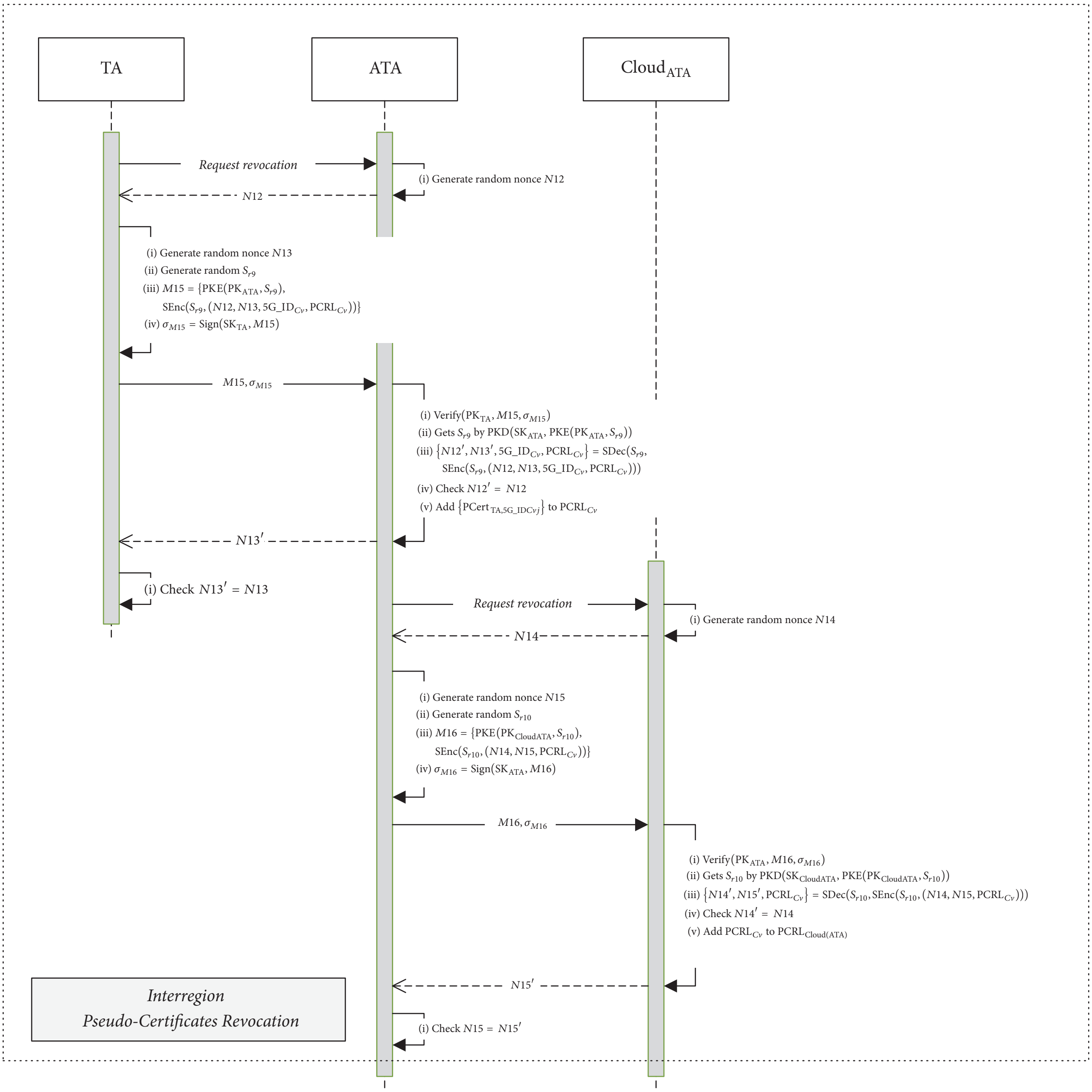

TA
ATA
$\text{Cloud}_{\text{ATA}}$
Request revocation
(i) Generate random nonce $N12$
$N12$
(i) Generate random nonce $N13$
(ii) Generate random S_{r9}
(iii) $M15 = \{\text{PKE}(\text{PK}_{\text{ATA}}, S_{r9}),$
$\text{SEnc}(S_{r9}, (N12, N13, \text{5G\_ID}_{Cv}, \text{PCRL}_{Cv}))\}$
(iv) $\sigma_{M15} = \text{Sign}(\text{SK}_{\text{TA}}, M15)$
$M15, \sigma_{M15}$
(i) $\text{Verify}(\text{PK}_{\text{TA}}, M15, \sigma_{M15})$
(ii) Gets S_{r9} by $\text{PKD}(\text{SK}_{\text{ATA}}, \text{PKE}(\text{PK}_{\text{ATA}}, S_{r9}))$
(iii) $\{N12', N13', \text{5G\_ID}_{Cv}, \text{PCRL}_{Cv}\} = \text{SDec}(S_{r9},$
$\text{SEnc}(S_{r9}, (N12, N13, \text{5G\_ID}_{Cv}, \text{PCRL}_{Cv})))$
(iv) Check $N12' = N12$
(v) Add $\{\text{PCert}_{\text{TA,5G\_ID}Cvj}\}$ to PCRL_{Cv}
$N13'$
(i) Check $N13' = N13$
Request revocation
(i) Generate random nonce $N14$
$N14$
(i) Generate random nonce $N15$
(ii) Generate random S_{r10}
(iii) $M16 = \{\text{PKE}(\text{PK}_{\text{CloudATA}}, S_{r10}),$
$\text{SEnc}(S_{r10}, (N14, N15, \text{PCRL}_{Cv}))\}$
(iv) $\sigma_{M16} = \text{Sign}(\text{SK}_{\text{ATA}}, M16)$
$M16, \sigma_{M16}$
(i) $\text{Verify}(\text{PK}_{\text{ATA}}, M16, \sigma_{M16})$
(ii) Gets S_{r10} by $\text{PKD}(\text{SK}_{\text{CloudATA}}, \text{PKE}(\text{PK}_{\text{CloudATA}}, S_{r10}))$
(iii) $\{N14', N15', \text{PCRL}_{Cv}\} = \text{SDec}(S_{r10}, \text{SEnc}(S_{r10}, (N14, N15, \text{PCRL}_{Cv})))$
(iv) Check $N14' = N14$
(v) Add PCRL_{Cv} to $\text{PCRL}_{\text{Cloud(ATA)}}$
$N15'$
(i) Check $N15 = N15'$
Interregion
Pseudo-Certificates Revocation

Figure 7: Interregion Pseudo-Certificates Revocation Protocol.

the valid private keys, pseudonymous certificates. Therefore, forged video upload is not possible.

Replay Attack. Replay attacks are avoided using timestamps or handshaking using random nonces. Lightweight timestamps technique is used in communications among DMV, TA, and LEA, since they are trusted entities that can easily have a synchronized clock. On the other hand, a handshaking using random nonces is used in communication between C_v and TA (in handover protocol), TA and ATA (in handover protocol), Cloud_{TA} and LEA (in video search protocol), and DV_i and Cloud_{TA} (in Official Vehicle Registration protocol) since it is hard to have a synchronized clock between those entities.

Nonseparation of Responsibilities between LEA and TA. The proposed scheme provides a separation of responsibilities between LEA and TA. This security mechanism will allow only LEA to manage the mapping of the unique identity of DV_i and $\text{5G\_ID}_{\text{DV}i}$. On the other hand, by using S_{r2} encrypted with PK_{TA} the confidentiality of $\text{Cert}_{\text{TA,5G\_IDDV}i}$, $\text{SK}_{\text{ABE(TA,DV}i)}$ is maintained from LEA. This mechanism avoids any privileged insider inside LEA to impersonate an official vehicle DV_i.

Table 1: Comparison of security and functionality features.

Feature	Eiza-Ni-Shi Scheme	Proposed scheme
Authentication and nonrepudiation	Yes	Yes
Conditional anonymity and privacy	Yes	Yes
Traceability	Yes	Yes
Management of multiple trusted authorities	No	Yes
Protection against DMV impersonation attack	No	Yes
Protection against forged video upload	No	Yes
Separation of responsibilities between LEA and TA	No	Yes
Protection against privileged insider attack in LEA	No	Yes
Protection against LEA impersonation attack	No	Yes
Exposure of location of official vehicles	No	Yes
Management of multiple TAs	No	Yes

Privileged Insider Attack in LEA. Since LEA receives $\text{Cert}_{\text{TA,5G\_IDDV}i}$, $\text{SK}_{\text{ABE(TA,DV}i)}$ encrypted with S_{r2} (only known as the official vehicle), LEA cannot obtain such values. This mechanism avoids any privileged insider inside LEA to impersonate an official vehicle DV_i.

LEA Impersonation Attack. LEA impersonation attack is avoided using the principles of public key cryptography. The Official Vehicle Registration request message $M3$ is accompanied with its digital signature σ_{M3} signed by the private key of LEA. The TA can verify the origin of the message since it can verify the authenticity of σ_{M3} using the public key of LEA PK_{LEA}.

Sybil Attack. To execute this kind of attack, the attacker must have nonrevoked, nonused, nonexpired, and authentic pseudo-certificates since the Cloud Platform verifies the validity (pseudo-certificate must not be revoked and expired) and authenticity (issued by the valid TA) of the pseudo-certificate attached to the video upload message. First, the attacker can try to listen to the network to capture a valid pseudo-certificate to reuse it later. However, this scenario is not a problem since the Cloud Platform has $\text{UPCL}_{\text{Cloud(TA)}}$ verification making the reuse of valid pseudo-certificates impossible. On the other hand, the attacker also can try to access the set of pseudo-certificates stored in C_v; since the pseudo-certificates are stored in secure storage devices this kind of attack is not also possible. Finally, the attacker can also try to guess a valid pseudo-certificate. This scenario is also not feasible since the video upload message includes a signature signed by a private key; this means that the attacker must guess not only a valid, not used, and not expired pseudo-certificate, but also its private key. We believe that such scenario is not feasible.

Exposure of Location of Official Vehicles. The present scheme provides a simple solution for this issue. The exposure of location of official vehicles is avoided by encrypting them using the public key of the Cloud Platform. Since the location information can only be decrypted by the authentic cloud with the corresponding private key, the adversary cannot obtain such information.

Management of Multiple Trusted Authorities. The proposed scheme includes a novel handover protocol which is executed when a participating vehicle C_v goes to a different regional area controlled by another trusted authority. This mechanism will help the real implementation of the proposed service, adapted to the common administrative structure of entities grouped in different geographical/administrative regions.

4.5. Performance Analysis of the Proposed Solution.

Since the intention of this analysis is to compare the overhead generated by the new security and functionality features of the proposed scheme with the previous one, the present work has used the same benchmark environment as [7]. It means that all the benchmarks were executed on a computer with Intel Core i7-2600 3.4 GHz processor using Crypto++ library 5.6.2 [15].

Two overheads are calculated in this section. (1) First, the time overhead in video transmission protocol is calculated and it is compared with the previous work. As well as [7], the overhead of vehicle registration protocols is not calculated since the generation and storage of pseudonymous certificates and signing keys are executed only once a year during the vehicles' inspection or service registration and because it is not a critical overhead for the real-time video reporting service. (2) After that, we analyze the overhead generated in handover protocol. The overhead of handover protocol is calculated autonomously without comparison with the previous work since it is a novel feature included only in the proposed scheme.

4.5.1. Overhead Generated in Video Transmission Protocol.

Before making the overhead calculation, it is important to select the certificate scheme for authentication of reported videos. The proposed scheme suggests the usage of PASS [8] as the mechanism for authentication of videos uploaded to the Cloud Platform, not only because it has one of the lowest overheads in terms of time for signing, certificate validation, and signature verification (see Table 2), but also because it solves the limitation of BP [16]. However, other algorithms such as BP [16], ECPP [17], DCS [18], and hybrid one [19] can be considered. Table 2 shows the time required for generation

Table 2: Overhead for signing, certificate verification, and signature verification for Eiza-Ni-Shi Scheme and proposed scheme.

Certificate scheme	Signing time (ms)	Certificate verification time (ms)	Signature verification time (ms)	Total (ms)
BP	0.6	1.2	1.2	3
ECPP	0.6	18.9	1.2	20.7
DCS	1.2	14.7	14.1	30
Hybrid	0.6	$18.9 + 9N_{\mathrm{crl}}$	1.2	$20.7 + 9N_{\mathrm{crl}}$
PASS	0.6	14.7	1.2	16.5

N_{crl}: size of certificate revocation list.

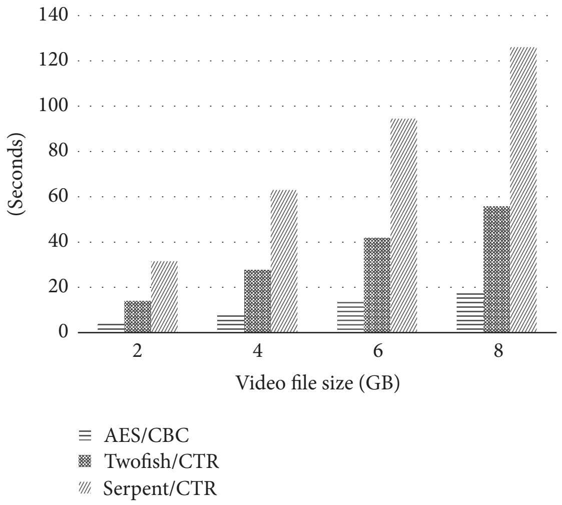


Figure 8: Symmetric encryption overhead using different algorithms.

and verification of signatures and certificate verification using different algorithms [8] (same for both Eiza-Ni-Shi Scheme and proposed scheme). The total overhead generated in video transmission protocol is composed of three elements: (a) video encryption, (b) video transmission, and (c) video decryption by official vehicles. It is important to mention that the overhead calculation of random number generation was omitted since it is a minimal value.

Video Encryption. The overhead calculation for video encryption was executed using the benchmark data delivered by [7]. Using such data, it is possible to deduce that the time required to perform the encryption operation $\mathrm{Ekw} = \mathrm{PEKS}(\mathrm{PK}_{R(\mathrm{TA})}, \mathrm{kw})$ is approximately 36.52 ms, the time required for the encryption process $\mathrm{ES}_{r6} = \mathrm{ABE.Enc}(\mathrm{PK}_{\mathrm{ABE(TA)}}, S_{r6}, \mathrm{Policy})$ is approximately 62 ms (with *Policy* containing 4 attributes), and the time required for signature generation $\sigma_{\mathrm{5G\_IDC}vj} = \mathrm{Sign}(\mathrm{SK}_{\mathrm{TA,5G\_IDC}vj}, \mathrm{hashValue})$ is approximately 0.6 ms using the PASS scheme where $\mathrm{hashValue} = h((h(U_{\mathrm{Cloud(TA)}}), \mathrm{ETV}_r, \mathrm{Ekw}, \mathrm{ES}_{r6}))$ (see Table 2). Additionally, the time required in executing $\mathrm{ETV}_r = \mathrm{SEnc}(S_{r6}, (\mathrm{TV}_r, \mathrm{Coordinate}_{Cv}))$ is illustrated in Figure 8, where the overheads for encryption of the video file are 455 MB/s when using AES/CBC, 147 MB/s when using Twofish/CTR, and 65 MB/s when using Serpent/CTR; all algorithms use 256-bit keys.

It is notorious that most of the overhead of this stage of the protocol is the symmetric encryption of the video file corresponding to $\mathrm{ETV}_r = \mathrm{SEnc}(S_{r6}, (\mathrm{TV}_r, \mathrm{Coordinate}_{Cv}))$ calculation. Since most of the overhead of this stage is the symmetric encryption of the video, the proposed system recommends encrypting the traffic accident video file while capturing it to minimize the time required for encryption before transmission.

Video Transmission. In the same way, the video transmission overhead calculation was based on data delivered by [7]. Such reference indicates that the estimated time required to upload/download the encrypted video file of 2 GB to/from the Cloud Platform using 5G communication is $T_{\mathrm{comm}} =$ 13.3 s assuming that the vehicle speed is 100 km/h and 5G connection speed is 1.2 Gbps. Based on this data, the video transmission protocol will require a total of 13.3 s for uploading 2 GB-size encrypted video by the participant vehicle and 13.3 s for downloading the same video by the official vehicles.

Video Decryption. The overhead calculation for video decryption was executed using the benchmark data delivered by [7]. Using such data, it is possible to deduce that the time required for $\mathrm{VerifySign}(\mathrm{PK}_{\mathrm{TA}}, \mathrm{PCert}_{\mathrm{TA,5G\_IDC}vj}, \sigma_{\mathrm{5G\_IDC}vj})$ is 14.7 ms when using the PASS scheme. The time required to execute $\mathrm{Verify}(\mathrm{PK}_{\mathrm{TA,5G\_IDC}vj}, (h(U_{\mathrm{Cloud(TA)}}), \mathrm{ETV}_r, \mathrm{Ekw}, \mathrm{Es}_{r6}), \sigma_{\mathrm{5G\_IDC}vj})$ step is 1.2 ms and the time required for $S_{r6} = \mathrm{ABE.Dec}(\mathrm{ES}_{r6}, \mathrm{SK}_{\mathrm{ABE(TA,DV}i)})$ is approximately 18 ms. Additionally, the time required in executing the decryption of the encrypted video ETV_r is similar to the ones shown in Figure 8. As well as in video encryption, most of the overhead of this stage of the protocol is the symmetric decryption of the encrypted video file.

Total Overhead of Video Transmission Protocol. As well as the previous work, the proposed scheme can report the traffic accident of the participant vehicle in less than a minute using AES/CBC cryptographic algorithm over a 2 GB video file assuming that the participating vehicle is encrypting the traffic accident video file while capturing it (the time required for encryption before transmission is reduced to a minimal value). As shown in Table 3, the additional overhead required by the proposed scheme compared to the Eiza-Ni-Shi Scheme is only the time required for one random number generation which is almost none in actual devices.

4.5.2. Overhead Generated in Handover Protocol. As well as in video transmission protocol, the steps related to random

Table 3: Total overhead of video transmission protocol when AEC/CBC is used and video size is 2 GB.

	Eiza-Ni-Shi Scheme	Proposed scheme
Video encryption	4.5099 s	4.5099 s + time for random number generation
Video transmission	13.3 s	13.3 s
Video decryption	4.5033 s	4.5033 s
Total	22,3132 s	22,3132 s + time for random number generation

Table 4: Handover protocol overhead.

Number of pseudo-certificates	Participating Vehicle Overhead (seconds)	TA Mediation Overhead (seconds)	ATA Response Overhead (seconds)	Total overhead (seconds)
24 (for a day)	0.0032	0.0215	0.0753	0.1239
48 (for 2 days)	0.0056	0.0263	0.1433	0.2231
168 (for a week)	0.0176	0.0503	0.4834	0.7192
720 (for a month)	0.0728	0.1607	2.0477	3.0012
2160 (for 3 months)	0.2168	0.4487	6.1287	8.9541
4320 (for 6 months)	0.4328	0.8807	12.2501	17.8836
8760 (for a year)	0.8768	1.7687	24.8331	36.2385

number generation were omitted for overhead calculation since their overhead is small and it is insignificant to the total overhead. On the other hand, the overhead calculation of message transmission was also omitted since its value is minimal assuming that 5G communication link is used among C_v, TA, and ATA.

For the calculation of overhead generated in handover protocol, we assume that TA and ATA communicate securely using the RSA algorithm (2048-bit key) while C_v authenticates with TA using the PASS [8] algorithm. The overhead calculation was based on Crypto++ 5.6.0 benchmarks [20, 21].

The total overhead of the handover protocol is composed of three components: (1) Participating Vehicle Overhead, (2) TA Mediation Overhead, and (3) ATA Response Overhead.

Participating Vehicle Overhead. This is the overhead generated by steps executed by C_v. In this part, C_v executes one public key encryption step, one symmetric key encryption step, one symmetric key decryption step, and one signing step using PASS. Assuming that random numbers, 5G_ID$_{CV}$, CoordinateC_v, and symmetric keys are 256 bits long, it is possible to deduce that the time required to perform $M7 = \{\mathrm{PKE}(\mathrm{PK}_{\mathrm{TA}}, S_{r4}), \mathrm{SEnc}(S_{r4}, (N3, N4, \mathrm{5G\_ID}_{Cv}, \mathrm{Coordinate}_{Cv}))\}$ is approximately 0.16 ms, the time required to execute $\sigma_{M7} = \mathrm{Sign}(\mathrm{SK}_{\mathrm{5G\_ID}Cvj}, M7)$ is 0.6 ms, and the time required to execute $\mathrm{SDec}(S_{r4}, M10)$ is approximately $(N/10)$ ms, where N is the number of pseudonymous certificates issued by ATA. In summary, the total overhead of participating vehicle is $((N/100) + 0.76)$ ms. Table 4 shows the calculation of the overhead with different number of issued pseudonymous certificates.

TA Mediation Overhead. This is the overhead generated by performing steps executed by TA. Here is the overhead calculation: the time required to perform $\mathrm{VerifySign}(\mathrm{SK}_{\mathrm{TA}}, \mathrm{PCert}_{\mathrm{TA,5G\_IDC}vj}, \sigma_{M7})$ is approximately 1.2 ms, the time required to execute $\mathrm{Verify}(\mathrm{PK}_{\mathrm{TA,5G\_IDC}vj}, M7, \sigma_{M7})$ is 1.2 ms, the time required to execute $\mathrm{PKD}(\mathrm{SK}_{\mathrm{TA}}, \mathrm{PKE}(\mathrm{PK}_{\mathrm{TA}}, S_{r4}))$ is approximately 6.08 ms, the time required to execute $\mathrm{SDec}(S_{r4}, \mathrm{SEnc}(S_{r4}, (N3, N4, \mathrm{5G\_ID}_{Cv}, \mathrm{Coordinate}_{Cv})))$ is less than 1 ms, the time required to execute $M8 = \{\mathrm{PKE}(\mathrm{PK}_{\mathrm{ATA}}, S_{r5}), \mathrm{SEnc}(S_{r5}, (N5, N6, \mathrm{5G\_ID}_{Cv}))\}$ is approximately 1.16 ms, the time required to execute $\sigma_{M8} = \mathrm{Sign}(\mathrm{SK}_{\mathrm{TA}}, M8)$ is 6.05 ms, the time required to decrypt $M9$ using S_{r5} is approximately $(N/10)$ ms, and the time required to perform $M10 = \mathrm{SEnc}(S_{r4}, (\{\mathrm{SK}_{\mathrm{ATA,5G\_IDC}vj}\}, \{\mathrm{PCert}_{\mathrm{ATA,5G\_IDC}vj}\}, \mathrm{PK}_{R(\mathrm{ATA})}, \mathrm{PK}_{\mathrm{ABE(ATA)}}, \mathrm{Policy}_{\mathrm{ATA}}, \mathrm{IP}_{\mathrm{Cloud(ATA)}}, U_{\mathrm{Cloud(ATA)}}, \mathrm{Reg}_{\mathrm{ATA}}, N4'))$ is approximately $(N/10)$ ms. In summary, the total TA Mediation Overhead is $((2N/10) + 16.69)$ ms. Table 4 and Figure 9 show the calculation of the overhead with different number of issued pseudonymous certificates.

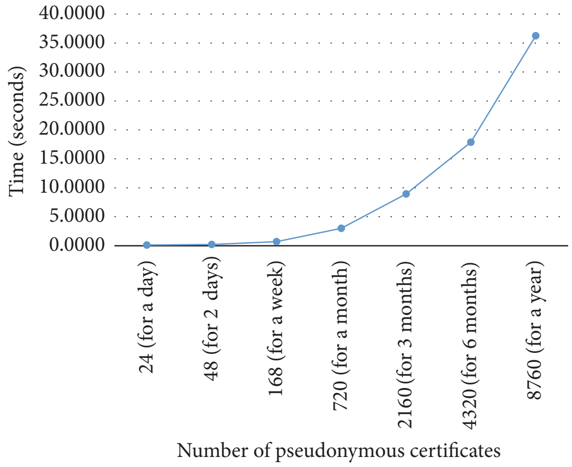


Figure 9: Total overhead of handover protocol according the number of issued pseudonymous certificates.

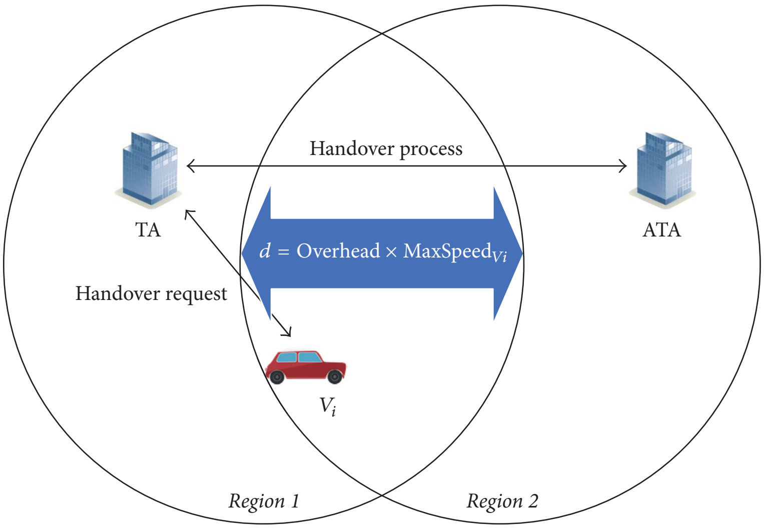


Figure 10: Relation between handover overhead and intersection zone.

Table 5: Distance of intersection zone.

Number of pseudo-certificates	Total overhead (seconds)	Distance (km)
24 (for a day)	0.1239	0.0069
48 (for 2 days)	0.2231	0.0124
168 (for a week)	0.7192	0.0400
720 (for a month)	3.0012	0.1667
2160 (for 3 months)	8.9541	0.4975
4320 (for 6 months)	17.8836	0.9935
8760 (for a year)	36.2385	2.0133

Corresponding data when MaxSpeed$_{Vi}$ = 200 km/h.

ATA Response Overhead. This is the overhead generated by steps executed by ATA. Here is the overhead calculation: the time required to perform $\mathrm{Verify}(\mathrm{PK}_{\mathrm{TA}}, M8, \sigma_{M8})$ is approximately 0.16 ms, the time required to execute $\mathrm{PKD}(\mathrm{SK}_{\mathrm{ATA}}, \mathrm{PKE}(\mathrm{PK}_{\mathrm{ATA}}, S_{r5}))$ is 6.08 ms, the time required to execute $\mathrm{SDec}(S_{r5}, \mathrm{SEnc}(S_{r5}, (N5, N6, \mathrm{5G\_ID}_{Cv})))$ is less than 1 ms, the time required to generate $\{\mathrm{SK}_{\mathrm{ATA,5G\_ID}Cvj}\}$, $\{\mathrm{PCert}_{\mathrm{ATA,5G\_ID}Cvj}\}$ is approximately $(2.734N)$ ms, and the time required to execute $M9 = \mathrm{SEnc}(S_{r5}, (\{\mathrm{SK}_{\mathrm{ATA,5G\_ID}Cvj}\}, \{\mathrm{PCert}_{\mathrm{ATA,5G\_ID}Cvj}\}, \mathrm{PK}_{\mathrm{R(ATA)}}, \mathrm{PK}_{\mathrm{ABE(ATA)}}, \mathrm{Policy}_{\mathrm{ATA}}, \mathrm{IP}_{\mathrm{CloudA(TA)}}, U_{\mathrm{Cloud(ATA)}}, \mathrm{Reg}_{\mathrm{ATA}}, N6'))$ is approximately $(N/10)$ ms. In summary, the total ATA Response Overhead is $(2.834N + 7.24)$ ms. Table 4 shows the calculation of the overhead with different number of issued pseudonymous certificates.

It is important to calculate the overhead generated in the handover protocol because the distance of the intersection zone of two regions depends on the overhead of handover protocol and the maximum speed of the participating vehicle (see Figure 10). In other words, the distance d is calculated as follows: $d = \mathrm{Overhead} \times \mathrm{MaxSpeed}_{Cv}$, where d is the distance of the intersection zone, Overhead is the total time overhead of the handover protocol, and MaxSpeed$_{Cv}$ is the maximum speed a participating vehicle can reach. The calculation of d is important for planning the coordinate of regions controlled by each trusted authority, since C_v needs to receive the pseudonymous certificates issued by ATA before exiting from its own region. If C_v has an accident in the intersection zone, the video is uploaded first in its own region and then it is uploaded to the region controlled by ATA (if the handover process is already finished). The minimum distance required for intersection zone of two regions when MaxSpeed$_{Vi}$ = 200 km/h is indicated in Table 5 and Figure 11.

Since the participating vehicles must renew the registration to the service annually, the number of pseudonymous certificates issued for handover should be much less than 8760 (for a year). We believe that certificates for 3 months should be enough for this purpose. If there is an extraordinary case when participating vehicle needs to stay in the region controlled by ATA for a long period of time, the participating vehicle can execute the handover protocol again when its pseudonymous certificate is running out. Assuming that the handover protocol is implemented with 2160 pseudonymous certificates the total overhead would be less than 9 seconds and d would be less than 0.5 km which would be very reasonable for real implementation.

4.5.3. Analysis of Region Organization. The intention of this subsection is to analyze the size of a region and the overhead caused by the handover protocol when a vehicle visits different number of regions.

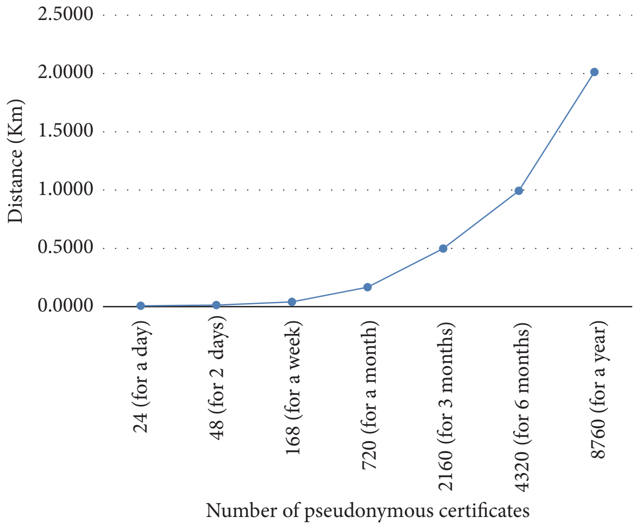


Figure 11: Minimum distance of intersection zone of two regions according to the number of issued pseudonymous certificates.

Size of a Region. It is very hard to determinate the size of a region since it depends on the needs of each country. But we recommend following the regulation of each country in administering the vehicle registration and driver licensing. For example, in the United States, there is an institution called Department of Motor Vehicles (DMV) which is a state-level government that administer vehicle registration and driver licensing. Since each country has similar departments, we recommend that each region for the proposed service must incorporate the geographical area controlled by a DMV, for example, an individual state for United States of America.

Overhead of Handover Protocol When Visiting Different Regions. For this analysis, we have taken the following assumptions: (1) the size of a region is determined by the geographical area controlled by a DMV, that is, an individual state, and (2) since we have recommended the usage of pseudo-certificate for three months (2160 pseudo-certificates) in handover protocol (in the previous subsection), we will use such values for this analysis.

Statistical data such as [22, 23] indicates that most of drivers use their motorized vehicles for activities of daily life, which means that they drive inside the same town most of the time. It means that most of participating vehicles will not execute or will rarely execute the handover protocol. However, for this analysis, we will consider all kinds of possibilities, including three kinds of vehicles: (1) ordinary vehicle which rarely leaves its region/state, (2) vehicles of people living in the border of a region/state which will make them visit the neighbor region/state frequently, and (3) extraordinary vehicles traveling several states frequently (e.g., interstate buses or cargo trucks).

For the first kind of vehicles (ordinary vehicles), the overhead caused by the handover protocol will be minimal since they will not execute or rarely execute such protocol. For the second kind of vehicles (living in a border), they will execute the handover protocol when visiting the neighbor region; however, the vehicle will not execute the handover protocol each time it crosses the border, but when all pseudo-certificates have been used or expired, that is, three months. In this second case, the overhead caused by the handover protocol will also be minimal since vehicles will execute the handover protocol (normally) every three months. Finally, Table 6 shows the overhead caused for the third kind of vehicles. Such data indicates the overhead generated when visiting different number of external regions every three months. For example, if a vehicle visits 5 different regions/states, it will spend a total of 44,77 seconds. We believe that the overhead of 44,77 seconds in three months is not a problem in implementing the proposed service. It is important to mention that the process is not executed during 44,77 seconds; instead C_v executes the 8,95 seconds' process each time it enters a new region.

Table 6: Handover protocol overhead when visiting several regions with pseudo-certificates for 3 months.

Number of different external regions visited by C_v	Total overhead (seconds)
1	8.95
2	17.90
5	44.77
10	89.54
20	179.08

This analysis has shown how the overhead caused in crossing different regions will not be a problem in implementing the proposed solution nationwide.

5. Conclusions

This paper has analyzed a pioneer research work proposing a novel system model for a 5G enabled vehicular network that facilitates a secure and privacy-aware video reporting service and it has found several security flaws and functionality limitations. Additionally, the presented work has proposed an improved scheme that delivers a trusted and reliable real-time video reporting service in 5G enabled vehicular networks which solves the identified security flaws and extends the functionality of the service for multiple trusted authorities. The security and performance analysis indicates how the proposed solution excels in security features and has reasonable overhead making it feasible for real implementation.

Notations

(i) Notations Used in Eiza-Ni-Shi Scheme

5G_ID:	Unique 5G identity for each vehicle
E:	Arbitrary entity
AS:	Set of attributes
$\mathrm{Cert}_{\mathrm{TA},E}$:	Public key certificate of entity E issued by TA
$\mathrm{dk}_{\mathrm{AS}}$:	Decryption key associated with the set of attributes AS

C_v:	Participating vehicle
DV_i:	Official designated vehicle i
TV_r:	Reported traffic accident video
Enc$C$:	Encrypted data of TV_r
kw:	Set of multiple keywords
$\mathrm{PK}_R/\mathrm{SK}_R$:	Public/private keys of the recipient R
$\mathrm{PCert}_{\mathrm{TA,5G\_ID},j}$:	Pseudonymous certificate of a vehicle, which is associated with 5G_ID, issued by TA for a period j
$\mathrm{PCert}_{\mathrm{TA},Cv,j}$:	Pseudonymous certificate of a vehicle C_v issued by TA for a period j
$\mathrm{PK}_{\mathrm{5G\_ID},j}/\mathrm{SK}_{\mathrm{5G\_ID},j}$:	Public/private keys of a vehicle, which is associated with 5G_ID, for a period j
$\mathrm{PK}_{Cv,j}/\mathrm{SK}_{Cv,j}$:	Public/private keys of a vehicle C_v for a period j
$\mathrm{PID}_{Cv,j}$:	Pseudo-identity of a vehicle C_v for a period j
$\mathrm{VP}_{Cv,j}$:	Validity period of pseudonymous certificate of vehicle C_v for a period j
$\sigma_{\mathrm{TA},Cv,j}$:	Digital signature of TA on the pseudonymous certificate of vehicle C_v for a period j
$\mathrm{SK}_{\mathrm{TA}}$:	Private key of TA for the purpose of signing the issued pseudonymous certificates
Tkw:	Trapdoor token associated with keyword kw
ΔT:	Validity threshold of a pseudonymous certificate
$\sigma_{\mathrm{5G\_ID},j}$:	Digital signature of a vehicle, which is associated with 5G_ID, for a period j
U:	Tag required to upload the video file to the cloud
$\mathrm{PK}_{\mathrm{ABE}}/\mathrm{MK}_{\mathrm{ABE}}$:	Public/master keys for CP-ABE algorithm.

(ii) Notations Used in the Proposed Scheme

Entities

C_v:	Participant vehicle
DV_i:	Official designated vehicle
DMV:	Department of Motor Vehicles
LEA:	Law Enforcement Agency
TA:	Trusted authority
ATA:	Away trusted authority
$\mathrm{Cloud}_{\mathrm{TA}}$:	Cloud Platform of TA.

Data

C_v:	Unique identification of C_v (C_v is used as representation of ID and entity)
$\mathrm{5G\_ID}_{Cv}$:	Unique 5G identification of C_v
DV_i:	Unique identification of DV_i (DV_i is used as representation of ID and entity)
$\mathrm{5G\_ID}_{\mathrm{DV}i}$:	Unique 5G identification of DV_i
$\mathrm{PK}_{\mathrm{DMV}}/\mathrm{SK}_{\mathrm{DMV}}$:	Public/private keys of DMV
$\mathrm{PK}_{\mathrm{LEA}}/\mathrm{SK}_{\mathrm{LEA}}$:	Public/private keys of LEA
$\mathrm{PK}_{\mathrm{TA}}/\mathrm{SK}_{\mathrm{TA}}$:	Public/private keys of TA
$\mathrm{PK}_{\mathrm{ATA}}/\mathrm{SK}_{\mathrm{ATA}}$:	Public/private keys of ATA
$\mathrm{PK}_{\mathrm{CloudTA}}/\mathrm{SK}_{\mathrm{CloudTA}}$:	Public/private keys of $\mathrm{Cloud}_{\mathrm{TA}}$
$S_{r1}, S_{r2}, S_{r3}, S_{r4}, S_{r5}, S_{r6}, \ldots, S_{rn}$:	Random symmetric keys
$\mathrm{TS}', \ldots, \mathrm{TS2}''''$:	Timestamps
$\Delta\mathrm{TS}$:	Timestamps expiration threshold
kw:	Keywords related to the reported video
$\mathrm{SK}_{\mathrm{TA,5G\_ID}Cvj}$:	Set of private keys issued by TA for C_v
$\mathrm{PK}_{\mathrm{TA,5G\_ID}Cvj}$:	Set of public keys stored inside pseudonymous certificates issued by ATA
$\mathrm{PCert}_{\mathrm{TA,5G\_ID}Cvj}$:	Set of pseudonymous certificates issued by TA for $C_v$with $\mathrm{5G\_ID}_{Cv}$
$\mathrm{SK}_{\mathrm{ATA,5G\_ID}Cvj}$:	Set of private keys issued by ATA for C_v
$\mathrm{PK}_{\mathrm{ATA,5G\_ID}Cvj}$:	Set of public keys stored inside pseudonymous certificates issued by ATA
$\mathrm{PCert}_{\mathrm{ATA,5G\_ID}Cvj}$:	Set of pseudonymous certificates issued by ATA for $C_v$with $\mathrm{5G\_ID}_{Cv}$
$\mathrm{PK}_{R(\mathrm{TA})}/\mathrm{SK}_{R(\mathrm{TA})}$:	Public key/private key of TA for Public Key Encryption with Keyword Search
$\mathrm{PK}_{R(\mathrm{ATA})}/\mathrm{SK}_{R(\mathrm{ATA})}$:	Public key/private key of ATA for Public Key Encryption with Keyword Search
$\mathrm{PK}_{\mathrm{ABE(TA)}}$:	Public key of TA for Attributed Based Encryption
$\mathrm{PK}_{\mathrm{ABE(ATA)}}$:	Public key of ATA for Attributed Based Encryption
$\mathrm{SK}_{\mathrm{ABE(TA,DV}i)}$:	Private key of DV_i issued by TA for Attributed Based Encryption
$\mathrm{SK}_{\mathrm{ABE(ATA,DV}i)}$:	Private key of DV_i issued by ATA for Attributed Based Encryption
Policy:	Policy of videos uploaded by C_v
$\mathrm{Policy}_{\mathrm{ATA}}$:	Policy of videos uploaded in $\mathrm{Reg}_{\mathrm{ATA}}$
$\mathrm{IP}_{\mathrm{Cloud(TA)}}$:	IP address of $\mathrm{Cloud}_{\mathrm{TA}}$
$\mathrm{IP}_{\mathrm{Cloud(ATA)}}$:	IP address of $\mathrm{Cloud}_{\mathrm{TA}}$
$U_{\mathrm{Cloud(TA)}}$:	Tag preagreed upon between TA and $\mathrm{Cloud}_{\mathrm{TA}}$
$U_{\mathrm{Cloud(ATA)}}$:	Tag preagreed upon between ATA and $\mathrm{Cloud}_{\mathrm{TA}}$
$\mathrm{Reg}_{\mathrm{TA}}$:	Region (coordinates) controlled by TA

$\mathrm{Reg}_{\mathrm{ATA}}$:	Region (coordinates) controlled by ATA
$\mathrm{Attribute}_{\mathrm{DV}i}$:	Attribute(s) of DV_i
$\mathrm{Cert}_{\mathrm{TA,5G\_IDDV}i}$:	Certificate issued by TA for DV_i with $\mathrm{5G\_ID}_{\mathrm{DV}i}$
$N1, N2, \ldots, Nn$:	Random nonces
$\mathrm{Coordinate}_{C_v}$:	Current GPS coordinate of C_v
TV_r:	Reported traffic accident video
PCRL_E:	Pseudo-Certificate Revocation List in an entity E
UPCL_E:	Used Pseudo-Certificate List in an entity E.

Functions

$\mathrm{PKE}(\cdot)$:	Public key encryption function
$\mathrm{PKD}(\cdot)$:	Public key decryption function
$\mathrm{SEnc}(\cdot)$:	Symmetric key encryption function
$\mathrm{SDec}(\cdot)$:	Symmetric key decryption function
$\mathrm{Sign}(\cdot)$:	Digital signature of a message
$Verify(\cdot)$:	Verifying a certificate
$VerifySign(\cdot)$:	Verifying a digital signature using a certificate
$\mathrm{ABE.Enc}(\cdot)$:	Attribute Based Encryption function
$\mathrm{ABE.Dec}(\cdot)$:	Attribute Based Decryption function
$\mathrm{PEKS}(\cdot)$:	Public Key Encryption with Keyword Search
$\mathrm{Trapdoor}(\cdot)$:	Trapdoor generation algorithm
$\mathrm{Test}(\cdot)$:	Test algorithm of Public Key Encryption with Keyword Search.

Conflicts of Interest

The author declares that they have no conflicts of interest.

References

[1] A. Gupta and R. K. Jha, "A survey of 5G network: architecture and emerging technologies," *IEEE Access*, vol. 3, Article ID 7169508, pp. 1206–1232, 2015.

[2] J. G. Andrews, S. Buzzi, W. Choi et al., "What will 5G be?" *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, Article ID 6824752, pp. 1065–1082, 2014.

[3] M. Irfan et al., "5G wireless technology – an overview of the current trends," *International Journal of Computer Applications Technology and Research*, vol. 5, no. 7, pp. 489–494, 2016.

[4] SK. Telecom, "SK Telecom 5G White Paper Ver. 1.0," SK Telecom, Seoul, Korea, White Paper, 2014.

[5] Samsung Electronics, "5G Vision," Samsung Electronics, Seoul, Korea, White Paper, 2015.

[6] NGMN., "NGMN 5G White Paper Ver. 1.0," MGMN, White Paper, 2015.

[7] M. H. Eiza, Q. Ni, and Q. Shi, "Secure and privacy-aware cloud-assisted video reporting service in 5g enabled vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, Article ID 7433471, pp. 7868–7881, 2016.

[8] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3589–3603, 2010.

[9] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Advances in Cryptology—EUROCRYPT 2004*, vol. 3027 of *Lecture Notes in Computer Science*, pp. 506–522, Springer, Berlin, Germany, 2004.

[10] J. Baek, R. Safiavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in *Proceedings of the Computational Science and Its Applications – ICCSA2018*, pp. 1249–1259, Perugia, Italy.

[11] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, IEEE, Berkeley, CA, USA, 2007.

[12] M. H. Eiza and Q. Ni, "An evolving graph-based reliable routing scheme for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 4, pp. 1493–1504, 2013.

[13] A. Alvez and D. Felton, "TrustZone: integrated hardware and software security. enabling trusted computing in embedded systems," ARM, White Paper. 2004.

[14] Freescale Semiconductors, "Security features in the i.MX31 and i.MX31L multimedia application processors," Freescale SEmiconducturs, White Paper, 2005.

[15] W. Dai, "Crypto++® Library 5.6.2 - a free C++ class library of cryptographic schemes. Crypto++," 2013, http://www.cryptopp.com/.

[16] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[17] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, Apr.)., ECPP, Efficient conditional privacy preservation protocol for secure vehicular communications. Presented ad INFOCOM, http://ieeexplore.ieee.org/xpl/articleDetails.jsp.

[18] A. Wasef, Y. Jiang, and X. Shen, "DCS: an efficient distributed-certificate-service scheme for vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 533–549, 2010.

[19] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proceedings of the VANET'07: Fourth ACM International Workshop on Vehicular Ad Hoc Networks*, pp. 19–28, Montreal, Canada, September 2007.

[20] Crypto++ 5.6.0 Benchmarks, 2016, https://www.cryptopp.com/benchmarks.html.

[21] D. He, C. Chen, S. Chan, and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions," *IEEE Transactions on Wireless Communications*, vol. 11, no. 1, pp. 48–53, 2012.

[22] E. Ericsson, *Driving pattern in urban areas – descriptive analysis and initial prediction model, Bulletin 185, Lunds Universitet*, 2000.

[23] United States Department of Transportation, "Bureau of Transportation Statistics," 2017, https://www.bts.gov.

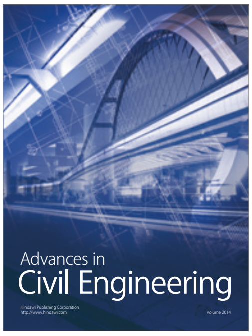
Journal of
Engineering

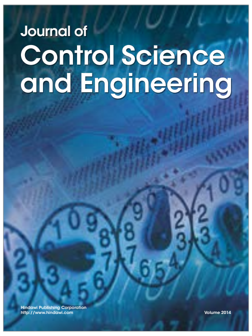
The Scientific
World Journal

International Journal of
Rotating
Machinery

Journal of
Sensors

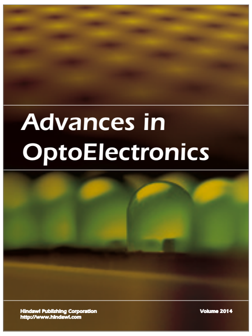
International Journal of
Distributed
Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

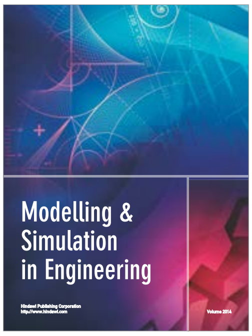
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

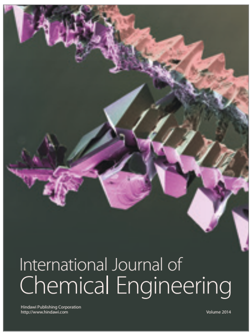

Advances in
OptoElectronics

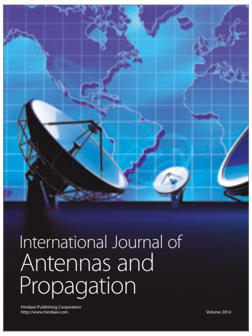
VLSI Design

International Journal of
Navigation and
Observation

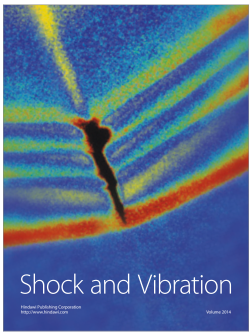

Modelling &
Simulation
in Engineering

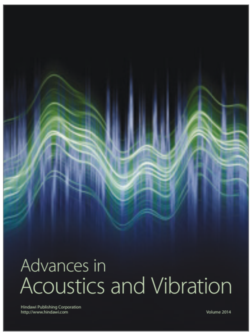
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration