SeVR^{+} :Secure and Privacy-Aware Cloud-Assisted Video Reporting Service for 5G Vehicular Networks

Atefeh Mohseni-Ejiyeh[1], Maedeh Ashouri-Talouki[2]
[1] Department of Computer Engineering,University of Isfahan, Isfahan, Iran
Email: atefeh_mohseni@eng.ui.ac.ir
[2] Department of Computer Engineering,University of Isfahan, Isfahan, Iran
Email: m.ashouri@eng.ui.ac.ir

***Abstract*—Recently, Eiza et al. proposed a secure and privacy-aware scheme for video reporting service in 5G enabled Vehicular Ad hoc Networks (VANET). They employ heterogeneous network and cloud platform to obtain more availability with low latency platform for an urgent accident video reporting service. In their study, for the first time the security issues of 5G enabled vehicular networks have been addressed. Eiza et al. claimed that their scheme guarantees user's privacy, confidentiality, non-repudiation, message integrity and availability for participant vehicles. In this paper, we show that Eiza et al. scheme is vulnerable to replay, message fabrication and DoS attacks. Regarding the sensibility of video reporting services in VANET, then, we propose an efficient protocol to overcome security weaknesses of Eiza et.al. scheme and show that the proposed protocol resists against commonplace attacks in VANET with acceptable communication and computation overhead.**

Keywords*—5G enabled Vehicular Network, Video reporting services, Cloud-Assisted, Security analysis, Message fabrication, DoS attack, Replay attack.

I. Introduction

Vehicular Ad Hoc Networks (VANETs) have been envisioned to enhance the passengers safety and comfort in the near future. Therefore, one of the potentially promising applications in VANETs is video reporting service which is aimed at delivering recorded videos from the camera mounted on a vehicle to coressponded officers. The camera records a video of an accident (or just for traffic monitoring) and reports it to the official vehicles like police, ambulance, etc. With respect to the necessity of providing desired QoS for video reporting services in VANETs, different solutions have been proposed. One of the most recent solution is exploiting 5G technologies [1].

5G is a promising technology started to be standardized by METIS project from 2012. Ambitious goals which are envisioned to attain more availability, flexibility and low latency in 5G cellular networks [2], attract researchers to overcome VANET challenges by enabling vehicles to communicate underlying fifth generation of cellular networks. [3]- [5].

To the best of our knowledge, Eiza et al. scheme [1] is the first study that addresses the security challenges of 5G enabled vehicular networks. In their scheme, a secure and privacy-aware video reporting service proposed for 5G-enabled vehicles. Moreover, their novel system, not only aimed to deliver videos instantly to official vehicles, by hiring cloud platform, but also protects users anonymity and privacy against internal and external adversaries. Although the authors claim the resilience of their scheme against common attacks, we have found that Eiza et al. scheme is vulnerable to replay, message fabrication and DoS attacks. Moreover, some security requirements such as non-repudiation and therefore traceability could be violated.

Hereby, in this paper, we explore Eiza et al. scheme's vulnerabilities and explain its problems. Furthermore, in order to overcome mentioned weaknesses, we propose a new authenticated scheme inspired by Eiza et al. protocol. Our scheme preserves additional security attributes which can be robust against potential attacks in 5G enabled vehicular networks.

The remainder of this paper is organized as follows. We review a state of the arts related studies in section II. Eiza et al.'s scheme discussed in section III and its vulnerabilities revealed in section IV. Then, the proposed protocol explained in section V and evaluated in section VI. Finally, section VII concludes our study.

II. Literatures review

As far as we know, Eiza et al. [1] is the first study which considere privacy and security requirements of 5G enabled vehicular networks for video reporting services. Previous studies mostly separated into two parts, security of fifth generation of cellular networks and secure and privacy-aware communication through VANET [6]- [9]. Hence, in the following we firstly introduce 5G cellular networks and its functionalities for vehicular networks then, review the related studies of secure video streaming either in the platform of 5G or VANET.

5G cellular networks aim to overtake 1,000 times higher mobile data rate with five times lower latency. Although, they are not currently achievable but it could be reached by utilizing heterogeneous network and additionally by using the combination of technologies such as D2D communication, milimeterWave (mmWave), visible light communication (VLC) and massive MIMO [10]. On the other hand, regarding the growing of high data-rate applications, in vehicular networks and the necessity of delay reduction specifically for public safety applications, 5G seems as a promising trend for VANETs.

Handling vehicular communications based on 5G technology has been noticed many researches not only in academia but also in industry world.Although, there are studies about the security issues in 5G such as [7] but, Eiza et al. is the first study

978-1-5090-5963-8/17/$31.00

in the context of security and privacy for 5G enabled vehicular networks. Moreover, data acceptance over the air interface via cloud is also a noticeable aspect of 5G. In the following, we particularly review the cloud assist video sharing services.

Liu et al. in [8] proposed a real time secure data sharing and searchable platform over video data which took both the advantages of the mobile cloud platform and the 5G technology simultaneously. Their scheme allows users to securely upload their real time videos and share them with whom they want immediately. Although, Liu et al.s scheme overcomes the security requirements but the communication and computation costs for mobile users are not efficient. In fact, because of using traditional encryption mechanism, users should always be online and do a huge computations to serve of proposed video sharing service [11].

Authors in [9], proposed an efficient cloud assisted framework for disseminating safety messages in VANET. The safety message should deliver to cloud by vehicle via corresponded gateway. Since the cloud knows the traffic flow and the geographic information of gateways, forwards the safety message to the gateway which is in the targeted area, however, the proposed framework for delivering safety message is similar to [1] but, they didnt address security issues in their study.

In the following we will review Eiza et al. protocol briefly. The important symbols used in Eiza et al. protocol has been listed in Table I.

TABLE I. NOTATION USED IN EIZA PROTOCOL

Notation	Notation
$5G\_ID$	Users identity(unique)
DV_i	The ith designated official vehicle
AS, dk_{AS}	A set of attributes and a decryption corresponded key
MS_{ABE}, PK_{ABE}	Master and public keys of $CP-ABE$ scheme
TV_r	The reported video of an accident
$PCert_{(TA,5G\_ID,j)}$	An issued pseudo-certificate for $5G\_ID$ in jth period
$\sigma_{(5G\_ID,j)}$	The digital signature of $5G\_ID$ in jth period
U	A verifiable tag for the cloud over video reports
ΔT	The validity threshold of certificates
kw	A set of keywords e.g. location of an accident, time, etc.
T_{kw}	corresponded trapdoor token with kw

III. REVIEW OF THE EIZA PROTOCOL

Eiza et al.'s protocol consists of registration, video transmission and video retrieval phases. Six major parts in their scheme are official vehicles (DV_i)[1], participant vehicles (C_v), Cloud Platform, Law Enforcement Agency (LEA), which is employed to trace misbehaving vehicles, Department of Motor Vehicles (DMV), which is supposed to authorize vehicles during registration phase, and Trust Authority (TA) which is responsible to generate and issue pseudo certificates for vehicles. Eiza et al.'s system model illustrated in Fig.1.

The main secure preliminaries employed in the Eiza et al. includes a pseudonymous authentication scheme with strong privacy preservation (PASS) [12], a public key encryption with a keyword search (PEKS) to enable saving encrypted videos in the cloud, Ciphertext-Policy Attribute-Based Encryption(CP-ABE) to enhance flexibility of retrieving private data by official

[1]That are served as an ambulance, police, traffic authority or etc.

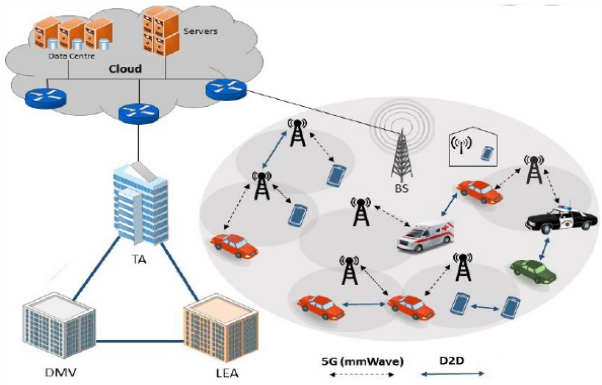

Fig. 1. Eiza et al.'s System Model in 5G enabled Vehicular Network [1]

vehicles, and a symmetric encryption algorithm $SEnc(.)$ to encrypt video reports. The details of Eiza et al.'s protocol will be explained in the following.

1) Registration phase: At the beginning of the protocol, participant and official vehicles should register through TA to participate in the service. Moreover, PASS scheme [12] which was adapted to use in Eiza et al. gives a set of issued pseudonymous certificates $\{PCert_{TA,5G\_ID,j}\}$ to corresponded C_v with an unique identity $5G\_ID$. Note that the number of certificates which are given to a participant vehicle is based on users regional properties.[2]

2) Video transmission: A participant vehicle during this phase uploads its recorded video to the cloudd platform.
Step 1. When a participate vehicle, C_v, records a video of an accident (TV_r), chooses a random symmetric encryption key S_{key}, then, encrypts it as follows $Enc_c \leftarrow SEnc(S_{key}, TV_r)$.
Step 2. C_v produces a searchable encryption by using the recipient public key PK_R and the key words set kw={accident video report,location,data and time} through $S_{PEKS} \leftarrow PEKS(PK_R, kw)$.
Step 3. Participate vehicle computes $ABE_c \leftarrow ABE.Enc(PK_{ABE}, S_{key}, Policy)$, in order to encrypt the encryption key S_{key} via CP-ABE scheme under policy Policy. Thereby, just recipient with private key dk_{AS} can decrypt this message and retrieve S_{key}.
Step 4. C_v signs the message$M = (Enc_c \parallel S_{PEKS} \parallel ABE_c \parallel h(U))$ by using its pseudonym certificate through $\sigma_{5G\_ID,j} = Sign(SK_{5G\_ID,j}, h(M))$ which $SK_{5G\_ID,j}$ is a private key of the selected certificate.
Step 5. C_v uploads generated message from step 1-4 as follows $\{Enc_c, S_{PEKS}, ABE_c, h(U), \sigma_{5G\_ID,j}, PCert_{5G\_ID,j}\}$ to the cloud platform. The video transmission phase is depicted in Fig. 2.

3) Video receipt: In this phase, an uploaded video to the cloud platform is being sent to the official vehicle.
Step 6. While a video is uploaded in the cloud, integrity of the $h(U)$ will be checked by the cloud platform first. Then, a notification sends to the nearest designated official vehicle DV_i with the content of

[2]For example, if user is located in the area which two accidents per day is possible to happen, 730 certificates are given to his/her for a year of subscribing in Eiza et al. service. Note that each certificate has a limited validity period ΔT.

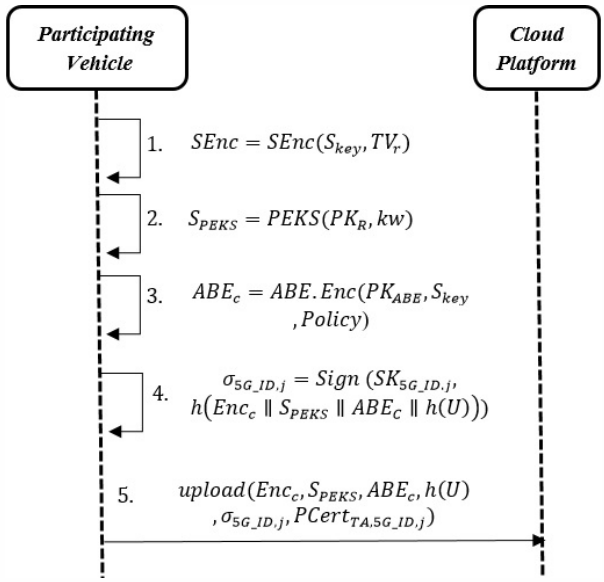

Fig. 2. Video transmission phase of Eiza et al. protocol

$\{Enc_c, S_{PEKS}, ABE_c, h(U), \sigma_{5G\_ID,j}, PCert_{5G\_ID,j}\}$.
Step 7. The validity of $PCert_{5G\_ID,j}$ will be verified by DV_i via checking whether $verify(P_{pub}, PCert_{5G\_ID,j}, \sigma_{5G\_ID,j})$ is held or not. If yes, DV_i extracts the value of public key $PK_{5G\_ID,j}$.
Step 8. Furthermore, the validity of the signature $\sigma_{5G\_ID,j}$ must be checked through $verify(PK_{5G\_ID,j}, h(M))$. If the signature is verified, DV_i goes to the next step.
Step 9. To extract the encryption key S_{key}, DV_i uses its decryption key associated with AS through $S_{key} \leftarrow ABE.Dec(ABE_c, dk_{AS})$.
Step 10. DV_i decrypts the received video by using S_{key} as follows $TV_r \leftarrow SDec(S_{key}, Enc_c)$. Fig. 3. illustrated the mentioned steps

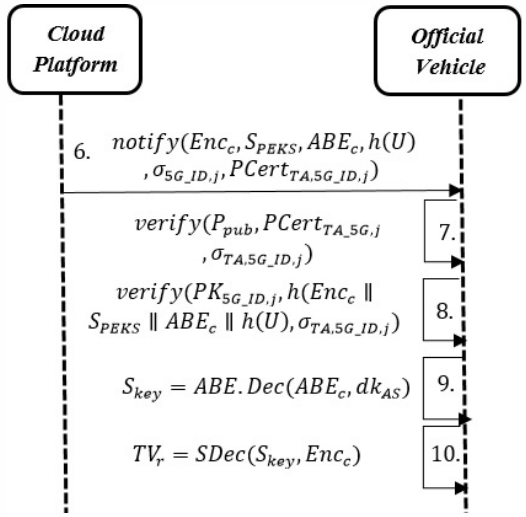

Fig. 3. Video Receipt phase of Eiza et al. protocol

4) Video retrieval: Since the videos are stored in the cloud for further checking by LEAs; the recipient that owns the private key SK_R works as follows:
Step 1. Whenever LEA needs to retrieve a video accident from the cloud, first set its desired keyword e.g. a specific location, then generates a searchable trapdoor through $T_{kwi} \leftarrow Trapdoor(SK_R, kw_i)$.
Step 2. T_{kwi} sent to the cloud platform via secure channel as a request.
Step 3. T_{kwi} will be checked by the cloud platform over ciphertext stored messages.
Step 4. If any matches found, the cloud platform sends the corresponded tuple $\{Enc_c, S_{PEKS}, ABE_c, h(U), \sigma_{5G\_ID,j}, PCert_{TA,5G\_ID,j}\}$ to LEA. The following steps for decrypting the video is similar to ones done by official vehicles. The described steps is depicted in Fig.4.

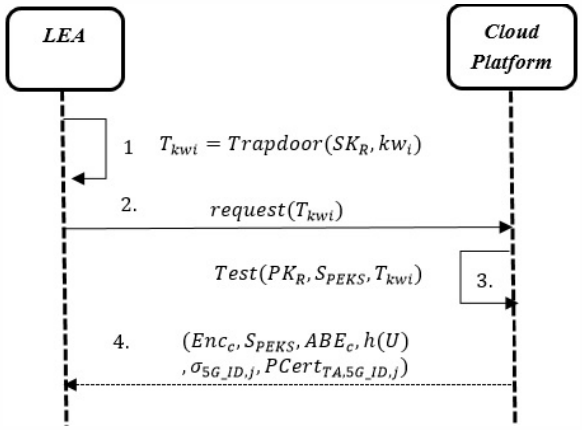

Fig. 4. Video retrieval phase of Eiza et al. protocol

IV. SECURITY WEAKNESSES OF EIZA PROTOCOL

In the following, we describe three vulnerabilities of Eiza et al.'s protocol.

A. Message fabrication attack

In Eiza et al.'s protocol, LEA is responsible for tracing internal adversaries whom sent fake videos. In this attack we show how an internal adversary uploads a fake video to the cloud which not only will be accepted by an official vehicle but also LEA cannot trace the sender of this fake video and cannot punish it consequently.

Let an internal adversary does not follow the protocol's rule in step 2 and uses nonsenses instead of legal (or predefined) values for kw or using a fake key instead of PK_R . Hence, because the official vehicle wont check the validity of S_{PEKS} through step 7-10, the report will be accepted by the official vehicle. Therefore, deceived official vehicle goes to manage the fake accident. After a while, when LEA wants to trace a malicious user, generates a trapdoor with legal kw (and intendent private retrieval key SK_R) through $Trapdoor(SK_R, kw_i)$ and sends it to the cloud platform for searching. Because of using invalid parameters by the adversary, despite of existence of fabricated video in the cloud, no video could be retrieved corresponded with LEA's query. Hereby, internal adversary not only sent a permissible fabricated message to the official vehicle and deceived it but also violets the traceability of a system which is a key feature of Eiza et al.'s scheme. This means their scheme does not ensure nonrepudiation.

B. Reply attack on Video Transmission Phase

In Eiza et al.'s scheme after receiving a video upload request in step 5, the cloud platform forwards it to the nearest official vehicle (step 6). Consider an adversary eavesdrops a packet which was sent through step 5 by a participant user and waits for a short time (to let cloud forwards corresponded notification to DV_i)[3]. Then re-uploads the sniffed packet in the cloud platform. Since, the cloud platform just checks the validity of $h(U)$, the message will be accepted and consequently the cloud sends a notification to the nearest official vehicle DV_j. Since, the certificate of re-uploaded message is verified during its validity period, each DV_i will follow the steps 7-10 to get the message is repeated; and in some cases that the video is new for DV_j, it will go to manage the fake accident. Hereby, the adversary could deceive official vehicles just by a simple replay attack. Due to the sensibility of the reporting service in vehicular networks and the urgency of the availability for the official vehicles in the Eiza et al.'s scheme, this simple attack can cause delay in service delivery by official vehicles and in worse case may affect peoples life where got injured in an accident. Additionally, this attack not only affect service availability but also disturbs the data stored in the cloud.

C. Denial of Service attack on Video Transmission Phase

As mentioned before, when a participant vehicle uploads an accident video to the cloud in step 5, the validity of the $h(U)$ will be checked by the cloud and upon verification, the corresponded notification will be sent to the nearest official vehicle. Let an external adversary captures a message of step 5 e.g. $\{Enc_c, S_{PEKS}, ABE_c, h(U), \sigma_{5G\_ID,j}, PCert_{5G\_ID,j}\}$. Because the value of $h(U)$ is not decrypted, the adversary can send a series of fake messages to the cloud platform with the valid tag $h(U)$. Hence, the cloud platform verifies each message (just by checking a simple hash value) and sends a notification to the nearest official vehicles. This attack makes corresponded official vehicles out of service, because it must do a huge computations per video reports. In fact, attaching the value of $h(U)$ does not guarantee that the user really knew the value of tag U and consequently is a legal user.

V. The Proposed scheme

In this section we suggest some solutions to empower Eiza et al.s scheme against above vulnerabilities. The proposed protocol is depicted in Fig. 5.

Step 1. The participant vehicle sends its registration request as follows $register - req = (C_v, 5G\_ID, PKE(P_{pub}, S_r)$.

Step 2. The DMV verifies the message and retrieves the C_v of participant vehicle then, forwards users request $(5G\_ID, PKE(P_{pub}, S_r))$ to TA.

Step 3. Similar to Eiza et al.'s protocol, TA generates a set of pseudonymous certificate $\{PCert_{TA,5G\_ID,j}\}$, where contains a private key SK_{5G_ID} a public key PK_{ABE} of an attribute based encryption scheme, a predefined policy set $Policy$, tag U, and a set of random numbers $r_{5G\_ID,j}$ then it encrypts them as $SEnc(S_r, (SK_{5G\_ID,j}, r_{5G\_ID,j}, PCert_{TA,5G\_ID,j}, PK_{ABE}, Policy, U))$. We will explain later that how these random numbers can prevent replay attack.

Step 4. DMV delivers received packet to the participant user.

Step 5,6. Official vehicle DV_i sends $(DV_i, 5G\_ID)$ as it's registration request to TA via LEA.

Step 7,8. TA produces a private key dk_{AS} based on the master key MK_{ABE} and issues a certificate $Cert_{TA,DV\_i}$ and sends to the DV_i through a secure channel.

Step 9. DV_i should register to the cloud platform to receive the related notifications of accident videos.

Step 10-12. These steps are done similar to Eiza et al.'s scheme steps 1-3 of video transmision phase.

Step 13. C_v selects a pseudo certificate $PCert_{5G\_ID,j}$ and produces its signature by using the related private key $SK_{5G\_ID,j}$ through $\sigma_{5G\_ID,j} = Sign(SK_{5G\_ID,j}, h(Enc_c \parallel S_{PEKS} \parallel ABE_c \parallel r_{5G\_ID,j} \parallel h(U)))$.

Step 14.In this step, C_v uploads its generated message to the cloud platform through $\{Enc_c, S_{PEKS}, ABE_c, r_{5G\_ID,j}, h(U), \sigma_{5G\_ID,j}, PCert_{5G\_ID,j}, H(*)^U\}$. Note that, $H(*)^U$ refers to a HMAC [4] function over all the message content by using U as a secret key.

Step 15. The validity of $h(U)$ and $H(*)^U$ first, is verified by the cloud platform and then, the cloud notification service will check whether the record indexed with $r_{5G\_ID,j}$ is already exists or not. In fact, the cloud platform allocates specific storage indexes related to the random generated numbers by TA for video reports. So if a report re-upload to the cloud, the cloud will ignore it. Otherwise, it sends a notification with the content of $\{Enc_c, S_{PEKS}, ABE_c, r_{5G\_ID,j}, h(U), \sigma_{5G\_ID,j}, PCert_{5G\_ID,j}\}$ to the nearest official vehicle.

Step 16-19. DV_i verifies the received video report similar to Eiza et al.'s scheme. In each step if the validity was not held, DV_i must report it to the nearest LEA through step20.

Step 20. If an abnormal behavior detected by DV_i , it reports to the LEA. Hence, in the proposed scheme, LEA does not refer to the cloud directly in order to trace misbehaving users.

Step 21-24. These steps are done similar to Eiza et al. scheme's steps 1-4 of video retrieval phase.

VI. Evaluation and results

In this section we analyze this proposed protocol in terms of security and efficiency. We show that how our solutions achieved noticable security resistance with minimum overhead on the communication and computation cost.

A. Performance evaluation of the proposed protocol

The proposed protocol compared to Eiza et al. have one more hash verification in the cloud platform and also running a random generator by the TA for the registration phase which can be done offline.

As mentioned before, assigning random number to each uploaded request will prevent replay attack. Therefore, cloud platform ignores two requests with the same random numbers. However, allocating specific storage for this service by the cloud may cause lost in some memory cells (because of those

[3]Note that, Eiza et al. adapted PASS scheme [12] in their protocol. In fact, original PASS scheme consider a short period of time for each certificate validity period e.g. about a few seconds. But, with Eiza et al. adaption and based on their service requirements, the validity period of each certificate is about at least a few hours.

[4]Keyed-hash message authentication code

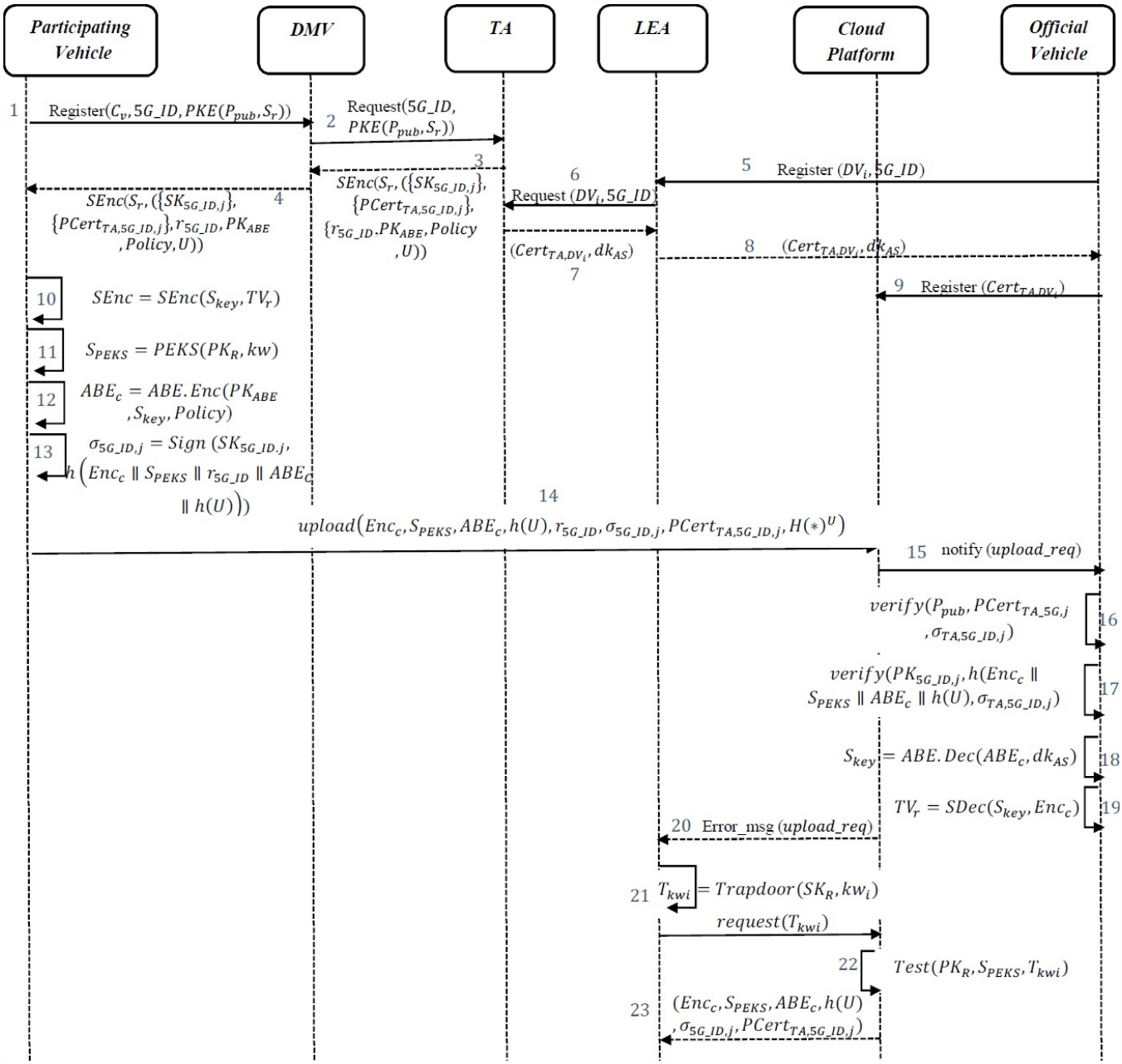

Fig. 5. The Proposed Protocol

unused pseudo-certificates) but in overall, and with respect to updating the service periodically, those unassigned memory cells could be reusable. In other words, employing random numbers might require more free memory spaces in the cloud at the start of running the service but, because of using each memory cell after a while, there is no memory lost in the proposed protocol. Note that, although using timestamp instead of random numbers might also prevent replay attack but in that way the protocol will be still vulnerable against DoS attack during the validity period of each issued certificate. So it is not an appropriate option for us.

B. Security verification of the proposed protocol

The proposed protocol is not only secure against attacks in [1] but it also guarantees the other security requirements described below:

1) Data confidentiality and integrity: The proposed protocol ensures data confidentiality and integrity. During the process of transmission, the recorded video first is encrypted by $SEnc_c(S_{key}, TV_r)$ and the encryption key S_{key} is transferred through an encrypted form. Thus the eavesdropper cannot retrieve any information from the transmitted data. Additionally, verifiable digital signature over videos ensures the integrity of the data and authenticity of its owner.

2) Conditional privacy and anonymity: By using PASS [12] scheme in this protocol, the privacy and anonymity of users are guaranteed until they are following the protocol honestly. In fact, to find a link between participants pseudo ID, the adversary has to find a collision in a one-way hash function which is impractical.

3) System availability and user Traceability: In order to ensure user traceability in the proposed protocol, when an official vehicle detects a fake reported video, it will send an error message to LEA instantly. So, the adversary is traceable in the proposed protocol even though the searchable encryption scheme which is used in the proposed protocol was vulnerable to inappropriate inputs such as keywords, because LEA does not refer to the cloud platform for downloading tampered video directly. In addition, the proposed scheme ensures systems availability similar to [1], by gaining 5G technologies and heterogeneous networks to delivering video report to the cloud platform as much fast as possible.

4) Resistance against man-in-the-middle attack: In order to resistant against man-in-the-middle attack, each packet signed with the participant's pseudo certificates private key. Thus, the message integrity and authentication is guaranteed as well.

5) Resistance against replay attack: To resist against replay attack, a random nonce is employed while sending an upload request to the cloud platform by the participant vehicle. So if the adversary tries to resend a captured packet, the packet will be ignored by the cloud platform. This feature also protects the protocol from DoS attack.

6) Resistance against participant/official vehicle impersonation attacks: Utilizing secure channel during the registration of official/participant vehicles and using digital signature for registration of participant vehicles, will ensure protocol is resistant against impersonation attack.

7) Resistance against DoS attack: Last but not least, in the proposed protocol, an internal adversary cannot send a series of fake video reports with a valid certificate because each certificate has a validity period, and in that period of time, only one random number is available for user to attach with its request. Any repeated message with the same random number will be ignored by the cloud platform. On the other hand, if an external adversary attaches a valid value of $h(U)$ to its packets, it will be dropped by the cloud platform because the validity of $H(*)^U$ also will be checked and because the adversary has no clue about the value of U, she cannot produce the correct value for its fake messages.

VII. Conclusion

Eiza et al. proposed a secure and privacy aware scheme for the first time based on 5G enabled vehicular networks which applied for video reporting service. Although, they claimed to propose a fully secure protocol, we found some weakness in their scheme which mostly comes from the behavoir of the cloud platform. Hence, we propose efficient solutions to overcome Eiza et al.'s security weaknesses and show that the proposed ptrotocol satisfies the common security requirements in such networks.

References

[1] 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, pp.7868 - 7881, 2016.

[2] O. Afif, et al, *Scenarios for 5G mobile and wireless communications: the vision of the METIS project*, IEEE Communications Magazine,vol.5, pp. 26-35, 2014.

[3] B. Bellalta, E. Belyaev, M. Jonsson and A. Vinel,*Performance evaluation of IEEE 802.11 p-enabled vehicular video surveillance system*, IEEE Communications Letters,vo.18, pp.708-711, 2014.

[4] H. He, H. shan, A. Huang and L. sun *Resource Allocation for Video Service in Heterogeneous Cognitive Vehicular Networks*, EEE Transactions on Vehicular Technology,pp.1-14,2016.

[5] F. Chiti, et al., *Communications Protocol Design for 5G Vehicular Networks*,5G Mobile Communications, Springer International Publishing,pp.625-649, 2016.

[6] M. Amoozadeh, et al. ,*Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Cooperative Driving*, IEEE Communications Magazine, vol. 53, pp. 126-132, 2015.

[7] Ericsson, *5G security scenarios and solutions*, Ericsson White paper,2015.

[8] J.K. Liu, et al.,*Secure Sharing and Searching for Real-Time Video Data in Mobile Cloud*, IEEE Network, vol.25, pp.46-50,2015.

[9] B. Liu, et al. ,*Cloud-Assfisted Safety Message Dissemination in VANET-Cellular Heterogeneous Wireless Network*, IEEE Systems Journal, pp.1-12,2015

[10] A. Jeffrey.G, et al. *What will 5G be?*,IEEE Journal on Selected Areas in Communications,vo.32, pp.1065-1082,2014.

[11] M.H. Au, K. Liang, J.K. Liu and R.Lu,*While Mobile Encounters with Clouds*, International Conference on Network and System Security, Springer International Publishing,2016

[12] Y. sun, et al. ,*An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications* ,IEEE Transactions on Vehicular Technology, vol.59, pp. 3589-3603, 2010.