Secure and Privacy-Aware Cloud-Assisted Video Reporting Service in 5G Enabled Vehicular Networks

Mahmoud Hashem Eiza, *Member, IEEE*, Qiang Ni, *Senior Member, IEEE*, and Qi Shi

***Abstract*—Vehicular networks are one of the main technologies that will be leveraged by the arrival of the future fifth generation (5G) mobile cellular networks. While scalability and latency are the major drawbacks of IEEE 802.11p and 4G LTE enabled vehicular communications, respectively, the 5G technology is a promising solution to empower the real-time services offered by vehicular networks. However, the security and privacy of such services in 5G enabled vehicular networks need to be addressed first. In this paper, we propose a novel system model for a 5G enabled vehicular network that facilitates a reliable, secure and privacy-aware real-time video reporting service. This service is designed for the participating vehicles to instantly report the videos of traffic accidents to guarantee a timely response from official and/or ambulance vehicles toward accidents. While it provides strong security and privacy guarantees for the participating vehicle's identity and the video contents, the proposed service ensures traceability of misbehaving participants through a cooperation scheme among different authorities. We show the feasibility and the fulfilment of the proposed reporting service in 5G enabled vehicular networks in terms of security, privacy and efficiency.**

***Index Terms*—5G Vehicular Networks, Cloud-Assisted, Security, Privacy-Aware, Video Reporting.**

I. Introduction

THE future fifth generation (5G) of cellular networks has recently attracted a noticeable amount of research interests and efforts in the academia and industry worldwide [1-3]. 5G is a promising technology that will not be just an increment of the current 4G technology, but offers a 1,000 times higher mobile data volume per unit area, 10-100 times higher number of connecting devices and user data rate, 10 times longer battery life, and five times reduced latency [4]. Recently, the Cisco Visual Networking Index report shows that monthly global mobile data traffic will be 30.6 exabytes by 2020 where 75% of this traffic will be video data [5]. Therefore, 5G cellular networks should be a paradigm shift in order to meet these increasing requirements and support hundreds of thousands of simultaneous connections for smartphones, wearable devices, smart vehicles, *etc*.

Mahmoud Hashem Eiza and Qi Shi are with the Department of Computer Science, Faculty of Engineering and Technology, Liverpool John Moores University, Liverpool L3 3AF, U.K. (e-mail: {M.Hashemeiza, Q.Shi}@ljmu.ac.uk).

Qiang Ni is with the School of Computing and Communications, Lancaster University, Lancaster LA1 4WA, U.K. (e-mail: Q.Ni@lancaster.ac.uk).

Despite a significant amount of research conducted on vehicular networks, *e.g.*, [6-9], they have not yet been realised or deployed on a large scale worldwide. The lack of scalability, high mobility support, latency requirements, and security and privacy issues are few examples of the difficulties facing a successful deployment of vehicular networks. Recent studies on the performance evaluation of both IEEE 802.11p and LTE standards, which are proposed for vehicular networking, show a lack of scalability and limited mobility support, in the case of IEEE 802.11p, while LTE standards struggle to obtain stringent delay requirements in the presence of high cellular network traffic [10-12]. With massive bandwidths, reduced latency and lowered cost, 5G enabled vehicular networks are a promising solution to empower the real-time services offered by vehicular communications especially in highly dense populated urban areas.

In order to address the challenging requirements facing the ambitious goals of 5G cellular networks, recent research and industry studies suggest that a potential multi-tier and heterogeneous network architecture along with the aggregation of the following three key radio technologies: millimetre wave (mmWave), ultra-densification of small cells, and massive multiple-input-multiple-output (MIMO), could help to achieve 5G goals [13, 4]. In addition to these 'big three' technologies, cloud-based networking, Software Defined Networking (SDN), Network Function Virtualisation (NFV), and Device-to-Device (D2D) communications are also expected to take place at the network level in 5G cellular networks. These network technologies may play a crucial role in facilitating the application of some of the aforementioned 'big three' technologies. For instance, in mmWave communications, link outages occur when obstacles such as buildings and freight vehicles block Line-Of-Sight (LOS) connection. In this case, D2D communications can maintain links between the communicating devices and mmWave base stations when LOS links are not available.

While the integration of the above-mentioned radio and network technologies can bring 5G cellular networks to fruition, a variety of security and privacy issues are imposed and thus should be carefully addressed. Methods of achieving security requirements such as identity protection and data integrity need to be revisited because of the expected heterogeneous network architecture in 5G networks. Concerning vehicular networks, although novel real-time applications can be realised using the futuristic 5G cellular network architecture, it should be considered that the generated data may be private and sensitive and yet relayed

through different network entities such as vehicles and small cells and/or storage in the cloud. This calls for an innovative design of secure and privacy-aware protocols for the potential real-time services in 5G enabled vehicular networks.

In this paper, we present a novel system model for 5G enabled vehicular networks that facilitates a secure and privacy-aware real-time video reporting service. To the best of our knowledge, this is the first study that envisages the architecture of 5G enabled vehicular network and addresses the security and privacy challenges of real-time video reporting services in such networks. The proposed service allows the participating vehicles to securely transmit videos of traffic accidents to the nearest designated official vehicle, *e.g.*, police or ambulance, over 5G communication links. The ultimate objective of this reporting service is to facilitate a timely response toward traffic accidents, which will lead to substantial improvements in road safety and potentially save more lives.

In order to gain people's attention and incentivise authorities to implement such a collaborative reporting service on the roads, a set of security and privacy requirements should be carefully addressed in the proposed 5G enabled vehicular networks system. The sender has to be provided with strong security and privacy guarantees against any attempt to trace the reported accident video via eavesdropping on the wireless communications or attacks on the small cells or hacking into the cloud. On the other hand, authorities and official vehicles should be able to confirm the authenticity of the reported video without revealing the identity of the sender. If the reported video looks suspicious or there is a legal need for authorities to identify the sender as a witness, who provided his/her consent for witnessing, cooperation among different authorities should commence to reveal the sender's identity.

Given the expected heterogeneous architecture of 5G enabled vehicular networks, the conflicting objectives of privacy and traceability, as well as the challenges of designing secure protocols for real-time services, we are motivated to design a novel secure and privacy-aware protocol that can effectively address these challenges. The new contributions of this paper are three folds.

- First, we propose a novel system model for 5G enabled vehicular networks. The proposed model shows the interactions among different radio and network technologies expected to be employed in 5G networks. Moreover, it highlights the security and privacy issues that emerge from the utilised 5G technologies in the context of 5G enabled vehicular networks.
- Secondly, we develop a secure and privacy-aware protocol that delivers a trusted and reliable real-time video reporting service in 5G enabled vehicular networks. The novelty of our proposed protocol lies in its unique design that targets the emerged security and privacy issues that will face the reporting service because of the small cells, D2D communications, and cloud-based networking in 5G networks. It incorporates a novel set of authentication and encryption schemes that is carefully designed to provide the security and privacy levels required for such a service. At the same time, the proposed protocol aims to minimise the overhead of these schemes and achieves the performance balance required to accommodate the real-time nature of the video reporting service.
- Finally, we design a secure and privacy-preserving registration scheme for the proposed reporting service that guarantees a distributed identity resolution of the participating vehicles. Furthermore, it ensures that insufficient corrupted authorities do not have the power to illegally reveal the identity of an innocent video sender.

Furthermore, the developed protocol can be extended and utilised by traffic management authorities to monitor the road conditions and nearby environments. The authorities can make use of a huge number of mobile and fixed cameras to collect real-time information for more efficient and effective management of roads. In this way, video reports could be sent upon request from authorities even if there is no traffic accident. However, in this paper, our focus is on promoting a secure and safe collaborative approach between vehicles on one-hand and traffic authorities on the other hand to deal with traffic accidents effectively. This collaborative service benefits from the attractive features that 5G cellular networks are expected to offer while addressing the security and privacy requirements of the participants. Thus, our work aims to take part in improving road safety and reducing the number of causalities that are caused by late response toward traffic accidents. We evaluate the proposed protocol through a comprehensive analysis to check its fulfilment and feasibility in terms of security, privacy and efficiency.

Although we choose the 5G technology to serve as a basic infrastructure to facilitate the proposed service, 4G LTE technology can be also utilised. However, besides the stringent delay requirements that have a great impact on preventing internal adversaries from tracking a particular vehicle while transmitting the accident video, as explained later in Section VI-A, 4G LTE networks do not offer the security requirements that can strengthen the application of the proposed service. User data integrity, accountability and non-repudiation for service requests, and protection against active International Mobile Subscriber Identity (IMSI) catching attacks are some examples of security requirements that are not offered by 4G LTE. These features are of great importance to improve the security and privacy aspects of the proposed reporting service and are foreseen to be addressed in 5G networks [14, 15]. Moreover, 5G is expected to offer users' applications the flexibility regarding their required security and privacy features. This flexibility means that a specific security and privacy policy, which is designed to protect the participating vehicles identities, can be applied in the proposed reporting service in 5G enabled vehicular networks.

The rest of this paper is organised as follows: Section II overviews the state of the art of the subject area. Section III presents the preliminaries that are relevant to this work. Section IV introduces the system model of 5G enabled vehicular networks. Section V presents the proposed secure and privacy-aware protocol. Security, privacy, and efficiency

analysis of the developed protocol is provided in Section VI. Finally, Section VII concludes the paper.

II. State of the Art

In order to guarantee a successful deployment and acceptance of the video reporting service in real-world scenarios, a set of security and privacy requirements such as authentication, non-repudiation, anonymity, as well as traceability should be met in accordance with the expected characteristics of the 5G network architecture. To the best of our knowledge, there are no previous studies that address these security requirements in the context of the futuristic 5G enabled vehicular networks. The security and privacy issues of 5G cellular networks and user privacy and anonymous communications in vehicular networks were studied separately. Next, we give a brief review of some related work.

In the context of security and privacy issues of 5G cellular networks, most studies focus on assessing the security challenges of individual technologies that are expected to coexist in 5G cellular networks where each one, *e.g.*, SDN or NFV, has its own security challenges and requirements. Mantas *et al*. [16] presented some representative examples of potential threats and attacks against the main components of 5G cellular networks. These examples were derived from the threats and attacks against the 3G and 4G mobile systems to highlight the future security issues in the upcoming 5G networks. The authors classified four attractive targets in the 5G network: User Equipment (UE), access networks, the mobile operator's core network and external IP networks. UE location tracking, message insertion attacks, physical tampering with Home eNode B (HeNB) femtocells, and eavesdropping on user data are few examples of the potential attack vectors that may face 5G networks' components.

In [17], the authors discussed the physical layer security for each of the 'big three' technologies proposed for 5G networks. Unlike the traditional approach, which protects data security through cryptographic techniques, physical layer security is identified as a promising strategy that provides secure wireless transmissions by smartly exploiting the imperfections of the communications medium. In this way, the quality of signal reception at unauthorised receivers can be effectively degraded, thus preventing them from acquiring confidential information from the received signal. The physical layer security does not depend on computational complexity and has high scalability that makes it an attractive option considering the different powers and computation capabilities of the connected devices in the 5G network. The authors proposed different physical layer security solutions for each of the 5G technologies, *e.g.*, artificial noise, antenna correlation and confidential broadcasting.

Alam *et al*. [18] proposed a security architecture to analyse security requirements for three types of D2D communications in LTE-A networks. They classified the use cases and scenarios of D2D communications, which are proposed in [19, 20], into three scenarios: 1) Network-covered D2D without user applications, where all devices in proximity are covered by a LTE-A network and user applications do not require D2D communications. This type is used for traffic offload purposes; 2) Network-covered D2D with user applications, where all devices in proximity are covered by a LTE-A network and user applications do require D2D communications. This type is used for social networking applications; and 3) Network-absent D2D for public safety, where at least one device in proximity is not covered by a LTE-A network. This type is used for disaster rescue. The authors defined the following four security attacks against the direct radio link in D2D communication: eavesdropping, impersonation attack, attack on traffic data and attack on control data. Based on the existing network security access functions and algorithms in LTE-A, the authors proposed authentication, key agreement, encryption and integrity procedures to protect the D2D communications in the aforementioned three scenarios.

In the context of vehicular networks, a handful of research work focuses on privacy-preserving and anonymous communications, *e.g.*, [21-25]. Sun *et al*. [26] proposed an identity-based security system for user privacy in Vehicular Ad-hoc Networks (VANETs) using pseudonym-based and group-signature-based authentication schemes to satisfy the security requirements of authentication, non-repudiation, message integrity and confidentiality while achieving privacy desired by vehicles and accountability required by authorities. The security system is proposed for safety messages broadcast where vehicles obtain a set of short-lived pseudonyms and renew them later via communications with the road side units (RSUs). The authors designed a threshold signature-based scheme to prevent corrupted or compromised authorities to frame an innocent vehicle. When a misbehaving vehicle is detected, all its pseudonyms will be revoked. This method results in a large certification revocation list (CRL) and all other vehicles within the same access group should update their information, which also results in high checking and updating overhead. Furthermore, if the RSU is compromised, the adversary will be able to link the issued pseudonymous certificates with the real identity of the targeted vehicle.

In [27], the authors proposed a collaborative protocol for enforcing anonymity in VANETs inspired by the well-known Crowds protocol [28] where each user probabilistically decides to send a message directly to a common receiver, or else to forward it to a peer, who is asked to repeat the process. The aim of the proposed protocol is to allow users to report traffic infractions where neither the infrastructure point nor the users participating in the protocol can compromise the anonymity of reporting users. When an accident occurs, the participating vehicle generates a message m that contains the description, location and time of the accident, encrypts m using the public key of the infrastructure point, and forwards it to a chosen neighbour. The message is then forwarded randomly until reaching its destination. The infrastructure point decrypts the received message and generates a hash $h(m)$ that is incorporated into a list of encrypted traffic offenses. This list is then made available to users to allow them to check whether their messages have been received or not. The main limitation of this protocol is the unconditional privacy, resulting in the traceability requirement unattainable. In this

way, users can easily deceive the authorities and generate fake traffic incident reports or even frame innocent vehicles.

Finally, Hu *et al*. [29] proposed ATCS, an anonymous and traceable communication scheme for VANETs that aim to provide anonymity, traceability and authenticity of signed broadcasting messages to prevent internal attacks. The ATCS is based on the efficient combination of the endorsing scheme using a group-based (*t*, *n*) threshold signature [30] and an anonymous signature scheme using Weil Pairing [31]. The anonymous signature scheme provides traceability in broadcast but cannot distinguish fake messages that might be generated by internal attackers. On the other hand, the endorsing scheme makes it possible to prevent internal attacks because each generated safety message *m* from vehicle C_v is endorsed, *i.e.*, authenticated, by other vehicles by generating their individual signatures of *m* if it is found to convey real information. After receiving enough individual signatures of *m* from other vehicles, C_v generates the integrated signature of *m* and broadcasts it. This scheme results in high signatures overhead because many vehicles should verify each broadcasted message before generating the final signature on *m* and broadcasting it.

Following the above discussion, it can be noticed that the proposed solutions for privacy and anonymous communications in VANETs focused on safety broadcast messages and assumed homogenous network architecture. Due to the nature of safety messages, their contents are meant to be seen by every entity that receives them. Moreover, they are periodically broadcasted to convey current information, so there is no benefit of storing these messages for use later. Consequently, the privacy of the messages' contents and the untrusted storage issue have not been considered or discussed in the current literature. Therefore, we can argue that no direct work has been conducted to design a secure, privacy-aware and efficient video reporting service in heterogeneous network architecture such as 5G enabled vehicular networks, which is the subject of this paper.

III. PRELIMINARIES

In this section, we introduce the cryptographic mechanisms and schemes that are utilised as building blocks in our proposed protocol. The main notations used throughout this paper are given in Table I.

TABLE I – NOTATIONS

5G_ID	A unique 5G identity for each vehicle
TA	Trusted Authority
E	An arbitrary entity
AS	A set of attributes
$Cert_{TA,E}$	Public key certificate of entity E issued by TA
dk_{AS}	Decryption key associated with the set of attributes AS
d_{lv}	The distance travelled by a vehicle C_v without changing its velocity and lane
DV_i	The official designated vehicle i
TV_r	The reported traffic accident video
Enc_C	The encrypted data of TV_r
I	The secret information
Ψ_i	The secret share i
$ITHS_{\Psi i}(m)$	The individual threshold signature on message m using the secret share Ψ_i
$ITHV(ITHS_{\Psi i})$	The individual threshold signature verification of $ITHS_{\Psi i}$
kw	A set of multiple keywords
PK_R/SK_R	The public/private keys of the recipient R
$PCert_{TA,5G\_ID,j}$	A pseudonymous certificate of a vehicle, which is associated with 5G_ID, issued by TA for a period j
$PCert_{TA,Cv,j}$	A pseudonymous certificate of a vehicle C_v issued by TA for a period j
$PK_{5G\_ID,j}$ /$SK_{5G\_ID,j}$	The public/private keys of a vehicle, which is associated with 5G_ID, for a period j
$PK_{Cv,j}/SK_{Cv,j}$	The public/private keys of a vehicle C_v for a period j
$PID_{Cv,j}$	The pseudo identity of a vehicle C_v for a period j
$VP_{Cv,j}$	The validity period of pseudonymous certificate of vehicle C_v for a period j
$\sigma_{TA,Cv,j}$	The digital signature of TA on the pseudonymous certificate of vehicle C_v for a period j
SK_{TA}	The private key of TA for the purpose of signing the issued pseudonymous certificates
R_{Cv}	The communication range of a vehicle C_v
SH_1, SH_2	Two random hash seeds used to generate the pseudonymous certificate
$THS(m)$	The threshold signature on a message m
$THV(THS)$	The threshold signature verification performed by the TA
T_{kw}	A trapdoor token associated with keyword kw
ΔT	The validity period threshold of a pseudonymous certificate
κ_i	The secret key generated by E_i for the threshold signature scheme
$\sigma_{5G\_ID,j}$	The digital signature of a vehicle, which is associated with 5G_ID, for a period j
U	The tag required to upload the video file to the cloud
PK_{ABE}/MK_{ABE}	The public/master keys for CP-ABE algorithm

A. Pseudonymous Authentication Scheme

Let $(\mathbb{G}_1, +)$ and $(\mathbb{G}_2, \cdot)$ be two cyclic groups of prime order q and $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be an efficient admissible bilinear map. A trusted authority (TA) chooses a random generator $P \in \mathbb{G}_1$, two one-way hash functions $h(\cdot)$, *e.g.*, SHA-512, and $f(\cdot) : \{0, 1\}^* \rightarrow \mathbb{G}_1$ and a random master key $s \in \mathbb{Z}_q^*$. The TA then sets $P_{pub} = sP$ as its public key and publishes the system parameters $(\mathbb{G}_1, \mathbb{G}_2, q, P, e, P_{pub}, h(\cdot), f(\cdot), SEnc(\cdot), \Delta T)$ where $SEnc(\cdot)$ is a secure symmetric encryption algorithm and ΔT is the validity period threshold of an issued pseudonymous certificate. In this paper, we adopt the pseudonymous authentication scheme with strong privacy preservation (PASS) [32]. The TA generates a private key SK_{TA} for the purpose of signing an issued pseudonymous certificates $PCert_{TA,Cv,j}$ that belongs to vehicle C_v for a validity period j. The issued certificate contains the public key $PK_{Cv,j}$ of C_v (21 *bytes*), its pseudo identity $PID_{Cv,j}$ (20 *bytes*), the certificate validity period $VP_{Cv,j}$ (4 *bytes*), and the digital signature $\sigma_{TA,Cv,j}$ of the TA on this certificate (21 *bytes*). Hence, the total size of $PCert_{TA,Cv,j}$ is 66 *bytes*. C_v can have multiple such certificates.

The TA generates the pseudo identities (PIDs) of C_v based on a one-way hash-chain technology. Each certificate $PCert_{TA,Cv,j}$ is calculated based on two hash chains with two random hash seeds SH_1 and SH_2. Therefore, releasing SH_1 and SH_2 can revoke all the pseudonymous certificates of C_v and reveal the linkability among these certificates. In this way, the CRL size will be linear with the number of revoked vehicles and unrelated to the number of pseudonymous certificates the revoked vehicle held. Upon the receipt of SH_1 and SH_2, each entity E in the system can calculate all PIDs of the

pseudonymous certificates held by the revoked vehicle and drop the messages signed by these certificates. As explained later in Section V-A, the number of pseudonymous certificates each vehicle acquires for the proposed video reporting service is relatively small. Therefore, the calculated certificates can be stored in E to drop any message that is signed by the revoked vehicle. Finally, the TA securely delivers the private key set $\{SK_{Cv,j}\}$ and the pseudonymous certificate set $\{PCert_{TA,Cv,j}\}$ to C_v and stores the mapping relationship between the real identity of C_v, its PIDs and the corresponding SH_1 and SH_2.

The reason that we adopt the PASS scheme in our work is that unlike other pseudonymous authentication schemes such as BP [21], PASS optimises the CRL size to be linear with the number of revoked vehicles as explained above. For instance, 43,800 pseudonymous certificates are added to the CRL when one vehicle is revoked in the BP scheme [21]. Moreover, the PASS scheme achieves the lowest certificate verification overhead in comparison to other schemes such as the Efficient Conditional Privacy Preservation (ECPP) protocol [33] and Hybrid scheme [34] as explained later in Section VI-B.

We assume that the TA is trusted by all entities and the mapping tables are strongly protected. However, if the TA is compromised, the privacy is compromised as well. One way to avoid this scenario is to distribute the TA's responsibilities among multiple TAs for joint certificate issuing and management in such a way that no less than a set number of the TAs can jointly reveal the link between a pseudonym and its associated real identity. The design of such a TA role sharing solution is beyond the scope of this paper.

B. Public Key Encryption with Keyword Search

The public key encryption with a keyword search (PEKS) mechanism allows an entity E to outsource the storage of its encrypted data to another entity, *e.g.*, a storage server in the cloud, while maintaining the ability to search encrypted keywords, which are associated with the encrypted data, without compromising the security of the original data [35, 36]. The entity E starts by generating a searchable encryption S_{PEKS} of a set of multiple keywords $kw = \{kw_1, kw_2 \dots kw_z\}$ as follows $S_{PEKS} \leftarrow PEKS(PK_R, kw)$ where PK_R is the public key of a recipient R. It then uploads S_{PEKS} along with the encrypted data to the storage server. In order to search for the encrypted data on the storage server, R generates a trapdoor T_{kwi} that is associated with the keyword kw_i using his private key SK_R as follows $T_{kwi} \leftarrow Trapdoor(SK_R, kw_i)$ and sends it to the storage server. The received trapdoor T_{kwi} authorises a search process on the storage server where a test function $Test(S_{PEKS}, T_{kwi})$ is run on stored S_{PEKS} and returns true if $kw_i \in kw$. Following, the ciphertext associated with the keyword kw_i is returned to R for decryption.

C. Ciphertext-Policy Attribute-Based Encryption

Ciphertext-Policy Attribute-based Encryption (CP-ABE) is an asymmetric encryption technique to realise complex access control on encrypted data on a storage server and keep the data confidential even if the storage server is untrusted [37]. Let us assume the universe of attributes is defined to be {'police vehicle', 'ambulance', 'traffic authority', 'traffic law enforcement'}. Upon system initialisation, the TA issues a public key PK_{ABE} and a master key MK_{ABE}. The MK_{ABE} is utilised to produce a decryption key dk_{AS} for an entity E that is associated with a set of attributes, AS, that describes E, *e.g.*, 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 $Policy$, *e.g.*, $Policy$ = {'police vehicle' OR 'traffic authority'}, as $ABE_C \leftarrow ABE.Enc(PK_{ABE}, data, Policy)$. Thus, E can access the encrypted data and decrypts it as follows $data \leftarrow ABE.Dec(ABE_C, dk_{AS})$. In this way, other entities such as E` cannot access the encrypted data unless the set of attributes, $AS$`, for its decryption key $dk_{AS`}$ satisfies the specified policy $Policy$. If yes, it can also apply $data \leftarrow ABE.Dec(ABE_C, dk_{AS`})$.

D. Threshold Schemes based on Secret Sharing

The threshold schemes are utilised to distribute secret information, *e.g.*, a secret key, to multiple entities to eliminate power centralisation and a single point of failure [26]. Let I be the secret information that can be divided into d pieces $I_1 \dots I_d$ where the knowledge of any number kp or more of these pieces can recover I while the knowledge of $(kp - 1)$ pieces or less keeps I completely undetermined [38]. These schemes are usually referred to as a (kp, d) threshold scheme, which is computed based on polynomial interpolation.

IV. 5G Enabled Vehicular Networks System Model

In this section, we propose a system model for 5G enabled vehicular networks. Afterwards, we define the security requirements that should be fulfilled to facilitate a successful deployment of the proposed video reporting service.

A. System Model

Fig. 1 shows the proposed multi-tier 5G enabled vehicular network composed of HetNets, D2D communications, a cloud platform, Department of Motor Vehicles (DMV), TA, Law Enforcement Agency (LEA), as well as vehicles with 5G cellular connectivity. In the following, we briefly discuss the system components in Fig. 1 and explain their roles in the 5G enabled vehicular networks.

1) Heterogeneous Networks (HetNets)

In order to meet the increasing demands of higher data rates and raise the network capacity in 5G, two solutions have emerged: 1) reduce the size of cells; and 2) move toward the mmWave spectrum. By reducing the size of the cell, area spectral efficiency is increased through higher frequency reuse, while the number of users competing for resources at each base station (BS) decreases [39]. The ultra-densification of small cells leads to a higher number of connected devices and higher mobile data rates. Nonetheless, much more bandwidth is still needed. The mmWave communications can provide very high data rates since it operates over a vast amount of spectrum in the range of 30-300 *GHz* where wavelengths are 1-10 *mm*. Thus, densifying mmWave cells can produce huge gains and form backhauling for 5G cellular

networks. However, mmWave communications are not yet ready to be used in mobile communications since it suffers from a tremendous propagation loss and may be blocked by obstacles, as they require establishing LOS communications. These technical challenges are still under investigation and it is expected to be resolved before 2020 [40].

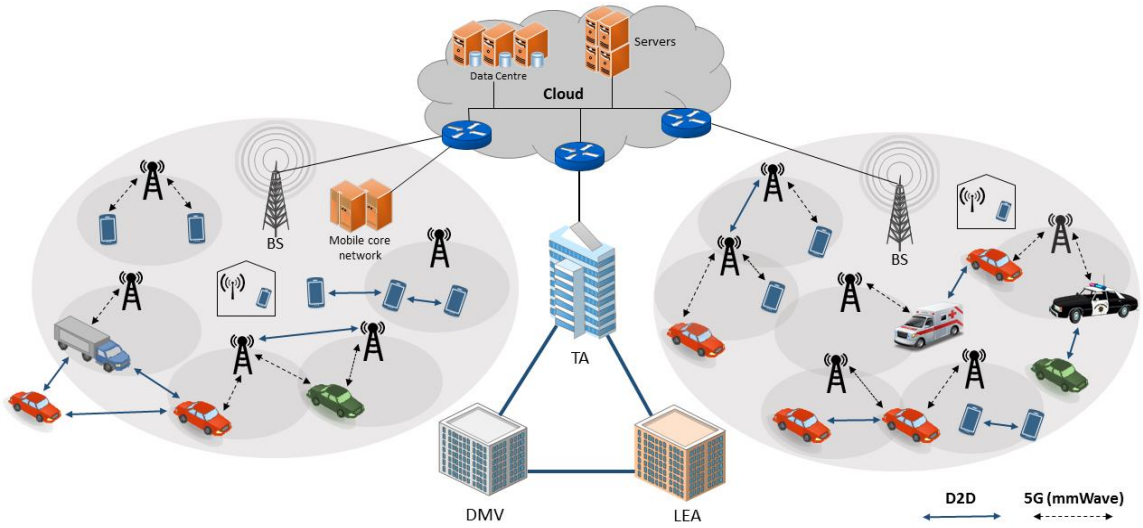

Fig. 1. 5G Enabled Vehicular Network – A multi-tier network model composed of macrocells, picocells, femtocells and D2D links

In Fig. 1, it is assumed that mmWave small cells provide data transmission over short-range mmWave links while a microwave BS, *i.e.*, a macrocell, provides control signals in microwave frequencies to ensure that control links are still in place. This approach is called 'soft cells' within the 3GPP standard [41, 42]. This means that vehicles should support associations with multiple radio access technologies that include not only 5G connectivity at mmWave frequencies but also 3G, 4G LTE, Wi-Fi, IEEE 802.11p and direct D2D communications. Choosing an appropriate standard and the right spectrum to utilise will be a complicated task in such a network [13]. This issue is beyond the scope of this paper. Besides the aforementioned small cells, a special type called Mobile femtocell (MFemtocell) is expected to be located within vehicles to communicate with drivers and passengers [43]. MFemtocell combines the mobile relay concept with the femtocell technology to accommodate high mobility users within public transport, *e.g.*, trains and buses, and private vehicles. In this way, users within vehicles receive high data rate services with reduced signalling overhead [44].

2) D2D Communications

Given the limitations of mmWave communications, D2D communication is an essential technology to support the 5G enabled vehicular network. D2D communication allows two nearby devices to communicate with each other in the licensed cellular bandwidth without a BS involved or with limited BS involvement [45]. D2D communication is currently considered as a part of 4G LTE-A standards in the 3GPP Release 12. In Fig. 1, vehicles can connect to the 5G cellular network via direct links with the mmWave small cells or by relay via other devices using D2D communication when LOS communications are not available. Besides that, D2D communication can be used to provide wireless connection between two small cells with a high data rate forming a part of the 5G backhaul where fibre links between them are not available. In Fig. 1, we assume that D2D communication is maintained with or without the BS control.

3) Cloud Platform

In Fig. 1, the cloud platform offers the capabilities of storing and accessing data from anywhere. This includes the reported videos of traffic accidents in our proposed service. The senders should transmit the reported videos to the cloud when a communication route to the recipient may not be available, *i.e.*, the official vehicle is not reachable via multi-hop communication. Therefore, moving the data to the cloud is essential to facilitate a quick notification and access to the recipient. In Fig. 1, we assume that a multipath reliable routing algorithm exists, *e.g.*, [46], to find multiple reliable routes from the sender to the cloud to transmit the video file as soon as possible. Moreover, it is assumed that the recipient can access the cloud instantly via 5G communications links.

Indeed, video flow processing could cause high loads on the servers that are processing and/or delivering the video data in the cloud. However, our proposed protocol only uses the cloud as a storage for receiving, storing and passing the video files to official vehicles. Thus, the cloud itself does not process the video files as they are encrypted. Although there are some emerging techniques for processing the encrypted files, they are resource demanding and inefficient. Nevertheless, to satisfy the high demands of 5G network users in general, it is assumed that the cloud platform implements specific solutions such as virtual video transcoding in the cloud [47] for higher-performance and higher-density video processing.

4) Trusted Authority (TA)

The TA is assumed to be fully trusted by all parties in the 5G enabled vehicular network system and in charge of registering the participating vehicles and conducting the

system initialisation. This includes the pseudonymous certificates generation, public/private key assignment, and creation of a database to store related information such as the pseudonym lookup tables. It is assumed that the TA is powered with sufficient storage capability, strongly protected and difficult for any adversary to compromise. Moreover, as explained later in Section V-B, we have devised a layer of role separation where the TA does not have the full mapping between the issued pseudonymous certificates and the real identity of the vehicle. This reduces trust reliance on the TA.

5) Department of Motor Vehicles (DMV)

All vehicles are supposed to register with the DMV where periodical inspection usually takes place. Besides the conventional identifier of the vehicle, *i.e.*, Electronic Licence Plate (ELP) or Electronic Chassis Number (ECN), each vehicle is assumed to have a 5G identifier (5G_ID), which is similar to the idea of a subscriber identification module (SIM) number in 3G and 4G systems. Therefore, each vehicle C_v registers with 2-tuple (C_v, 5G_ID) at the DMV. Furthermore, the DMV is assumed to be connected to a secure wired network where it can provide the TA with an updated list of the 5G identities of registered vehicles that have expressed their willingness to participate in the video reporting service.

6) Law Enforcement Agency (LEA)

Due to the sensitivity of the reported information, *i.e.*, traffic accidents, LEAs are part of the proposed system because they should be able to trace misbehaving users that might report fabricated accident videos. However, this privilege should not be used to unnecessarily track innocent vehicles that reported genuine accidents in the first place. This is not only because of the possibility of resulting in the reporting vehicle being abused but also to make sure that the driver and/or passengers of the reporting vehicle will not be asked to come as witnesses in court unless they have given their consent to do so. Thus, LEAs cannot reveal the identity of the reporting vehicle unless they cooperate with the DMV and the TA to do that as explained later in Section V.

B. Security Objectives

It can be seen in Fig. 1 that the proposed system has different network components where each one has different security issues. In the following, we describe the security objectives that should be fulfilled to achieve a reliable, secure and privacy-aware video reporting service in the 5G enabled vehicular networks shown in Fig. 1.

- Authentication. This requirement includes vehicle authentication and message integrity. Vehicle authentication enables the designated official vehicles and LEAs to check the authenticity of the sender, whereas message integrity ensures that the content of the reported video has not been altered in transit. All accepted video reports should come from the participating vehicles only and delivered unaltered.
- Non-Repudiation. The participating vehicles should not be able to deny the video reports generated by themselves. Non-repudiation is very important due to the sensitivity and consequences of the reported accident videos. In this way, malicious users will not be able to deceive the system without being identified.
- Conditional Anonymity and Privacy. Privacy is an essential requirement for the proposed reporting service to gain people's acceptance and participation. A vehicle owner's identity and location information are preserved against unlawful tracing and user profiling. However, the ability of revealing the identity of the reporting vehicle should be offered for the authorities only in special circumstances. In the proposed system shown in Fig. 1, the TA can partially reveal the real identity of a participating vehicle, whereas other entities could neither identify the real identity nor correlate the reported videos signed by the same sender in the long term. Using the pseudonymous authentication schemes, the conditional anonymity and privacy are held if the validity period of the pseudonymous certificate is less than a threshold ΔT.
- Traceability. This feature is required to identify malicious users who could transmit fake accident video reports. For liability purposes, LEAs need to reveal the identity information of the misbehaving participants and revoke their credentials. This is done to prevent these participants from further disrupting or deceiving the authorities' operations. Certain cooperation among different entities should take place for the purpose of tracing malicious and/or misbehaving participants as explained later in the protocol description in Section V.

C. Adversary Model

In the 5G enabled vehicular networks, we consider any component to be an adversary if it misbehaves or deviates from the legitimate operations required by the system. Due to the openness of wireless communications and the deployment of small cells in an unfenced environment, we take into account two kinds of adversaries: external and internal. The external adversary can capture the communications and analyse the transmitted packets between the communicating entities to learn about their identities, track their locations and learn about the contents of transmitted packets, *i.e.*, the traffic accident video. On the other hand, the internal adversary is either one of the network entities that has been compromised by an attacker or a misbehaving user. In our threat model, we consider that small cells, vehicles, DMV, LEA and the cloud platform are compromisable and therefore can act as an internal adversary. The internal adversary shares the same goals as the external adversary in which he/she aims to observe other vehicles' identities and locations and capture or alter the contents of the transmitted videos. In the following, we describe the main attacks that can be mounted by external and/or internal adversaries.

- Eavesdropping. This attack can be mounted against the mmWave and/or D2D wireless communication links in Fig.1 by installing receivers on the road to eavesdrop the messages transmitted by vehicles. The aim of this attack is

to analyse the transmitted data packets to infer the source and recover the contents of the transmitted data packets.

- Fabrication. The adversary can transmit a fabricated traffic accident video to deceive the authorities and affect the response of official vehicles and other users as well. This attack can be only mounted by internal adversary. As explained later in Section V, only the participants can upload the video files to the cloud after encrypting and signing these files. Thus, the external adversary cannot directly mount this attack.
- Traffic analysis. This attack can be mounted by either an external or internal adversary with the aim of identifying the source of the transmitted packets and consequently tracking the vehicle that reported the traffic accident. This attack presents a major violation of the participating vehicles' privacy.

Other threats such as compromising the cloud storage, impersonation, and framing attacks can be also considered in our threat model. In the following sections, we explain how the proposed protocol can resist such threats in the context of the 5G enabled vehicular network shown in Fig. 1.

V. Secure and Privacy-aware Video Reporting Service Protocol

In this section, we develop the secure and privacy-aware video reporting service protocol in 5G enabled vehicular networks. In the following, we describe the operations of the proposed protocol in detail as shown in Fig. 2.

A. System Initialisation

In the proposed system, the TA is assumed to manage a certain regional area that could be a state or a city or a district. The TA chooses ΔT as the validity period threshold of the pseudonymous certificates that will be issued to each participating vehicle. Since these certificates will be only used for the purpose of reporting traffic accident videos, the TA estimates the number of pseudonymous certificates that a vehicle needs to acquire. We assume that each vehicle should have enough pseudonymous certificates for a whole year until the next vehicle's inspection. Let us assume that A_r is the maximum number of traffic accidents the participating vehicle could report every day. In this way, the number of pseudonymous certificates for the whole year will be $365 \cdot A_r$ certificates. If we assume that the participating vehicle might report two accidents per day, *i.e.*, $A_r = 2$, then 730 pseudonymous certificates will be needed for the whole year, which amounts to nearly 48 *KB* given that the certificate size is 66 *bytes* as illustrated before in Section III-A. Therefore, it is sufficient from a storage point of view to store this number of certificates in the participating vehicle.

It is guaranteed that the issued pseudonymous certificates, which are stored in each participating vehicle, cannot be used to impersonate several vehicles in order to mount a Sybil attack because each certificate has a specific validity period and the number of certificates is relatively small.

B. Participants and Official Vehicles Registration

A new registration scheme is designed to allow a vehicle C_v to participate in the proposed service and be assured that no entity will be able to reveal its identity as long as the reported traffic accidents are authentic. The registration of the participants and official vehicles commences as follows.

- *Step* 1. During the vehicles annual inspection, the user expresses its willingness to participate in the video reporting service. The participant vehicle registers its 2-tuple (C_v, 5G_ID) with the DMV and includes a random symmetric key $S_r \in \mathbb{Z}_q^*$, which is encrypted using the TA's public key P_{pub}, expressed as $PKE(P_{pub}, S_r)$.
- *Step* 2. The DMV passes the registration request with the encrypted symmetric key to the TA requiring a set of pseudonymous certificates for the participating vehicle for the purpose of the reporting service. The DMV only sends the 5G_ID of the participating vehicle to the TA. The mapping between the vehicle real identity and its 5G_ID is kept at the DMV. This will offer a layer of role separation and more protection for the real identity of the participating vehicle as to be discussed later. It should be noticed that the 5G_ID is not necessarily fixed for a particular vehicle and can be changed during the next inspection/registration event.
- *Step* 3. Based on the request received from the DMV, the TA issues a set of pseudonymous certificates $\{PCert_{TA,5G\_ID,j}\}$, a set of private keys $\{SK_{5G\_ID,j}\}$, a policy *Policy* = {'police vehicle' OR 'ambulance' OR 'traffic law enforcement' OR 'traffic authority'}, and a tag $U \in \mathbb{Z}_q^*$, which will be used by the participating vehicle to upload the reported video to the cloud. The tag U is a pre-agreed value between the TA and the cloud platform and it is not unique to a participating vehicle. When the cloud receives a video file that is tagged with U, it saves the file and notifies the registrant official vehicles. In this way, the participating vehicles are not required to register with the cloud for the proposed reporting service. Finally, the TA encrypts all this information using the decrypted symmetric key S_r and sends them back to the DMV as $SEnc(S_r, (\{SK_{5G\_ID,j}\}, \{PCert_{TA,5G\_ID,j}\}, PK_{ABE}, Policy, U))$. Here, PK_{ABE} is the public key that will be used by the participant to encrypt a one-time encryption key S_{key} under *Policy* using CP-ABE as explained later in *Step* 12.
- *Step* 4. The DMV forwards the encrypted information to the participating vehicle.

In this way, the DMV knows the vehicle's 5G_ID and its real identity but not its issued pseudonymous credentials. On the other hand, the TA knows the 5G_ID identity and the corresponding pseudonyms but not the real identity of the participating vehicle. Furthermore, only the participating vehicle can decrypt the received message in *Step* 4 and gets the set of pseudonymous credentials. Thus, this prevents external adversaries from mounting impersonation attacks by stealing the pseudonymous credentials of legitimate participating vehicle.

Finally, the received information is stored within a tamper-proof device (TPD) that each participating vehicle is assumed to be equipped with to store the cryptographic information mentioned above. The TPD is a device that provides secure storage of cryptographic information and sensitive data as well as accelerating and securing cryptographic operations [48]. The implementation cost of the TPD is assumed to be the responsibility of the DMV.

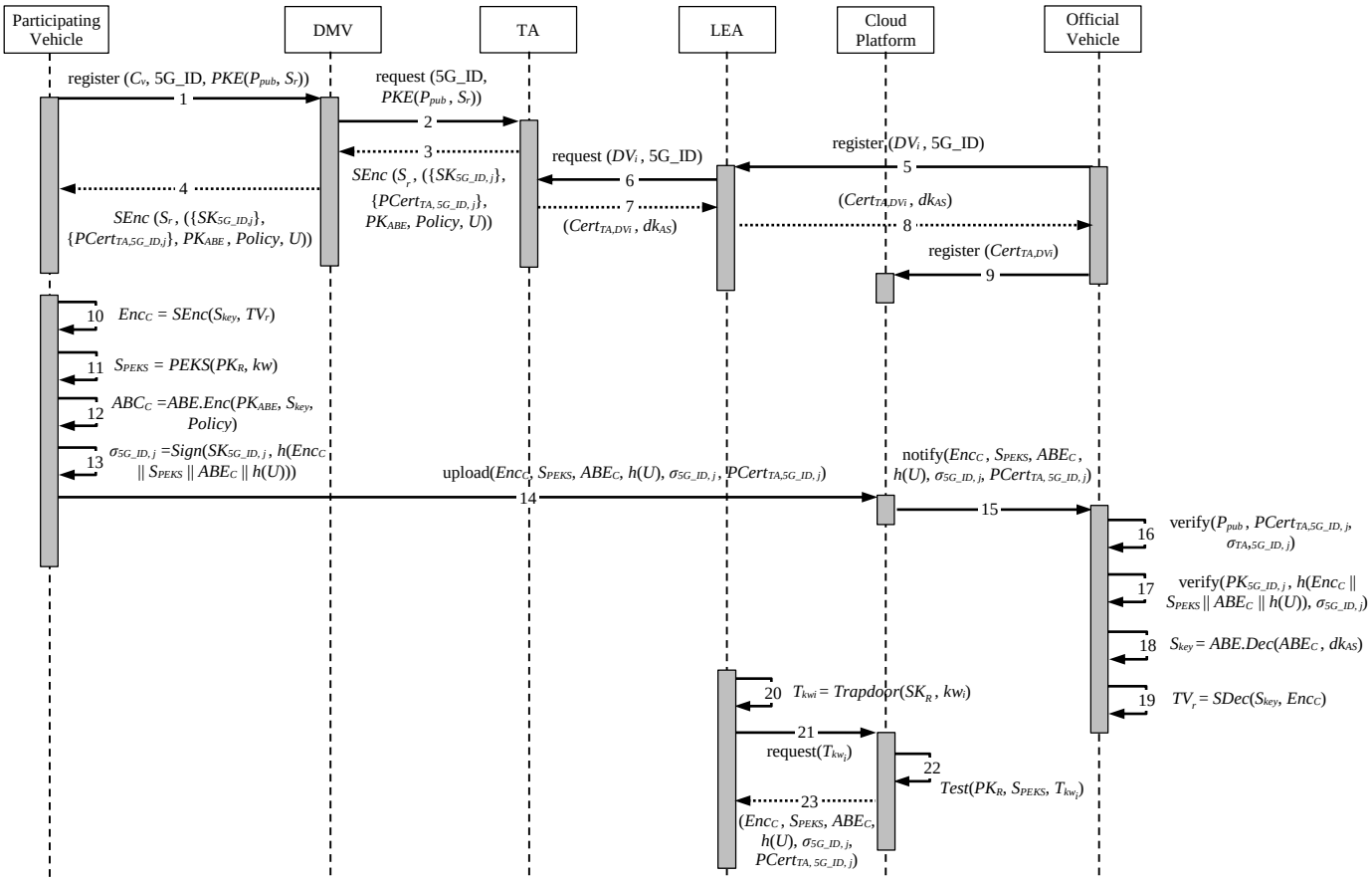

Fig. 2. The Proposed Secure and Privacy-aware Video Reporting Protocol

- *Steps* 5, 6. The official vehicles should also register to be part of this service. This is necessary to ensure that only designated official vehicles will receive the notification of a reported traffic accident video. A designated official vehicle DV_i sends a request to the TA via the LEA to register and gets a digital certificate and a decryption key.
- *Steps* 7, 8. After verifying the request, the TA issues the certificate $Cert_{TA,DVi}$ for DV_i and uses the master key MK_{ABE} to produce a decryption key dk_{AS} that is associated with the following set of attributes, AS = {'police vehicle', 'ambulance', 'traffic law enforcement', 'traffic authority'}. This information is then delivered to the DV_i's TPD via LEA. It should be noticed that the set of attributes in AS can be tuned based on the type of official vehicle, *i.e.*, police or ambulance. In this work, we assume that all official vehicles should have an access to the traffic accident video.
- *Step* 9. DV_i uses the received information to register with the cloud platform to receive notifications when an encrypted traffic accident video file, which is tagged with U, is uploaded to the cloud storage. We assume that the registrant official vehicles would receive notifications that are related to the regional area managed by the TA in Fig. 1. Distributing notifications from different regional areas that are under the management of different TAs is beyond the scope of this paper and is left for future work.

It should be noticed that the registration process of participating vehicles is not performed in real-time. It takes place at the DMV at the annual inspection of vehicles or whenever a vehicle decides to participate. The same case is applied to the official vehicles at a specific LEA. Additionally, we assume that the registration process is performed over a secure wired network thus there is no need to encrypt the registration messages in *Steps* 1, 2, 5, 6, 7, 8 and 9 in Fig. 2. Otherwise, these messages can be protected using suitable encryptions methods. Note that *Steps* 5-9 are independent of *Steps* 1-4 although they are shown in the same figure with consecutive message numbers. This also applies to the other message groups in Fig. 2.

At the end of the registration process, the TA chooses the signing key SK_{TA}, which has been used to sign the issued pseudonymous certificates, to be distributed. It computes the SK_{TA}'s shares Ψ_i where $i = 1 \ldots d$ and distributes these shares among d different entities, *e.g.*, the DMV and multiple LEAs.

Once a share Ψ_i is received, the corresponding entity generates a secret key κ_i that will be jointly utilised with Ψ_i to generate the partial threshold signature as explained later.

C. Video Transmission

- *Step* 10. When an accident occurs, the participating vehicle C_v acquires the recorded video file through its cameras and starts the video uploading process. First, it generates a one-time encryption/decryption key S_{key} for the symmetric encryption algorithm $SEnc(\cdot)$ and uses it to encrypt the accident video report TV_r as follows $Enc_C \leftarrow SEnc(S_{key}, TV_r)$ where Enc_C is the ciphertext of TV_r.
- *Step* 11. C_v uses PK_R, the public key of the recipient R, to produce a searchable encryption of the keyword set kw = {"accident video report", location, date and time} as follows $S_{PEKS} \leftarrow PEKS(PK_R, kw)$. The set kw can be extended to include more keywords but it is advised to keep the number of keywords small to avoid delays that may occur in the search process.
- *Step* 12. C_v utilises the CP-ABE to encrypt the one-time symmetric key S_{key} under *Policy* as follows $ABE_C \leftarrow ABE.Enc(PK_{ABE}, S_{key}, Policy)$. In this way, only the recipient with the decryption key that complies with *Policy* can decrypt ABE_C and retrieve S_{key}.
- *Step* 13. Using its selected pseudonymous certificate, C_v signs the tuple $\{Enc_C, S_{PEKS}, ABE_C, h(U)\}$ as follows $\sigma_{5G\_ID,\,j} = Sign(SK_{5G\_ID,j}, h(Enc_C \parallel S_{PEKS} \parallel ABE_C \parallel h(U)))$, where $SK_{5G\_ID,j}$ is the C_v's private key associated with the selected certificate and '||' denotes data concatenation.
- *Step* 14. C_v uploads $\{Enc_C, S_{PEKS}, ABE_C, h(U), \sigma_{5G\_ID,j}, PCert_{TA,5G\_ID,j}\}$ to the cloud platform over the 5G enabled vehicular network using the available communication links, *i.e.*, mmWave and D2D communication links as shown in Fig. 1. It can be noticed that, besides the cloud platform and the TA, the tag U is only known to the participating vehicles. The adversaries cannot capture U by mounting eavesdropping and/or traffic analysis attacks since it is encrypted in *Steps* 3 and 4 and, based on the one-way property of hash functions, its value cannot be retrieved using $h(U)$ in *Step* 14 or *Step* 15.

D. Video Receipt/Retrieval

- *Step* 15. Once the uploading process is done and the cloud platform verified the $h(U)$ value, the notification service notifies the nearest designated vehicle DV_i and sends it the following tuple $\{Enc_C, S_{PEKS}, ABE_C, h(U), \sigma_{5G\_ID,j}, PCert_{TA,5G\_ID,j}\}$. We assume that the location information of the official vehicles is updated periodically in the cloud. This assumption is valid since the location of an official vehicle DV_i is not a secret at this stage. However, since the location information of police vehicles could be interesting to criminals, one possible solution is to let the cloud platform informs the police control centre that can then instruct relevant police vehicles to retrieve the data from the cloud. This solution however needs more investigation and is left for future work.
- *Step* 16. DV_i verifies the received certificate $PCert_{TA,5G\_ID,j}$ as follows $verify(P_{pub}, PCert_{TA,5G\_ID,j}, \sigma_{TA,5G\_ID,j})$. If $PCert_{TA,5G\_ID,j}$ is proved to be valid, DV_i extracts the public key $PK_{5G\_ID,j}$ of the sender from the certificate.
- *Step* 17. DV_i verifies the received signature $\sigma_{5G\_ID,j}$ as follows $verify(PK_{5G\_ID,j}, h(Enc_C \parallel S_{PEKS} \parallel ABE_C \parallel h(U)), \sigma_{5G\_ID,j})$.
- *Step* 18. If $\sigma_{5G\_ID,j}$ is successfully verified, DV_i uses its decryption key dk_{AS} to decrypt the symmetric encryption key as follows $S_{key} \leftarrow ABE.Dec(ABE_C, dk_{AS})$.
- *Step* 19. DV_i uses S_{key} to decrypt the ciphertext and retrieve the traffic accident video file TV_r as follows $TV_r \leftarrow SDec(S_{key}, Enc_C)$.

In our proposed protocol, the encrypted traffic accident videos stay on the cloud storage to be retrieved whenever they are needed. Later on, a designated recipient LEA who can search for the traffic accident videos on the cloud, *i.e.*, the recipient R with the pair PK_R/SK_R, can retrieve the required videos as follows.

- *Step* 20. LEA generates the searchable trapdoor token T_{kwi} as follows $T_{kwi} \leftarrow Trapdoor(SK_R, kw_i)$, where keyword kw_i can be a location, a date, or just "accident video report".
- *Step* 21. LEA sends this token T_{kwi} to the cloud platform, assuming that there is a secure channel between them.
- *Step* 22. The receipt of T_{kwi} authorises the search process over the ciphertext at the cloud.
- *Step* 23. LEA receives the corresponding tuple $\{Enc_C, S_{PEKS}, ABE_C, h(U), \sigma_{5G\_ID,j}, PCert_{TA,5G\_ID,j}\}$ if the search was successful. Finally, LEA uses the same procedure mentioned above to retrieve the video file TV_r.

VI. Security, Privacy and Efficiency Analysis

A. Security and Privacy Analysis

1) Authentication and Non-Repudiation

In the proposed service, the authentication and non-repudiation are achieved by using a public key based digital signature that binds an encrypted traffic accident video to a pseudonym and consequently, to the real identity of the sender. As shown in *Step* 14 in Fig. 2, the sender attaches his/her pseudonymous certificate $PCert_{TA,5G\_ID,j}$ to the uploaded file. $PCert_{TA,5G\_ID,j}$ includes the sender's public key and the TA's signature as explained in Section III-A. In this way, the recipient can authenticate the sender by verifying its digital signature, to ensure the integrity and authenticity of the uploaded video file as shown via *Steps* 16 and 17 in Fig. 2.

2) Conditional Anonymity and Privacy

Our proposed protocol is resilient to traffic analysis attacks and achieves the conditional anonymity and privacy of the sender by using the pseudonymous authentication technique. As pointed out before, this technique conceals the real identity of the sender and makes it infeasible for other network entities and/or adversaries to identify the sender of a specific message.

Therefore, even if the cloud platform is compromised, the adversary will not be able to reveal the identity of the sender by looking at $PCert_{TA,5G\_ID,j}$ unless the adversary has access to the mapping information of $PCert_{TA,5G\_ID,j}$ and SH_1 and SH_2 used to generate the pseudo identities of this sender at the TA.

In addition, the sender C_v is required to use a different pseudonymous certificate for each new reported traffic accident video. Note that these pseudonymous certificates are only used for this reporting service, while for broadcasting safety or other messages, C_v should use different certificates. Thus, it is infeasible to track C_v by correlating the public keys it utilised. Let us assume the following scenario where an internal adversary controls at least two small cells separated by a distance d_{sc} and is able to capture all the data packets of a transmitted video file from C_v. The adversary can correlate two utilised public keys if C_v is driving at constant velocity V_{Cv} in the same direction on the same lane for duration T_{st} between the two compromised small cells.

Let the vehicle transmission range be R_{Cv} = 500 *m*, its constant velocity V_{Cv} = 100 *km*/*h*, T_{st} = 25 seconds, the size of TV_r is 2GB, and distance d_{lv} within which C_v does not change its velocity or lane. C_v can avoid being tracked if it finishes transmitting the video file TV_r using the same key before travelling a distance equal to $(2R_{Cv} + d_{lv})$ between the two observation points. After T_{st} = 25*s*, C_v travels d_{lv} = 695 *m* with V_{Cv} = 100 *km*/*h*. According to the latest connection speed tests for 5G wireless technologies, an uninterrupted stable connection of 1.2 *Gbps* in a vehicle travelling at 100 *km*/*h* is achieved [49]. In this case, the time needed to transmit TV_r is approximately 13.3*s* where C_v would have travelled approximately 370 *m* during this time without changing its velocity or lane. With the transmission range R_{Cv} = 500*m*, we can easily find that 370 < (2×500 + 695), *i.e.*, C_v cannot be tracked in this scenario. If $d_{sc} > (2R_{Cv} + d_{lv})$, C_v can avoid being tracked by changing the utilised key before travelling a distance equal to or longer than d_{sc}. Usually, in a traffic accident scene, vehicles would move slowly or even stop, particularly inside a city. Therefore, it will be guaranteed that the participating vehicle will finish transmitting the traffic accident video before travelling between the two observation points. Moreover, it is hard for the adversary to recognise the participating vehicle since many vehicles exist at the traffic accident scene.

It can be concluded from the above discussion that the high connection speeds and the low latency provided by the 5G enabled vehicular network have a great impact on preventing internal adversaries from linking different videos transmission to a particular vehicle and consequently revealing its identity. It is infeasible for the adversary to track the sender since the time needed to transmit the video file is very short. Therefore, the sender does not need to change its certificate while transmitting the same video file. Finally, it can be noticed from Fig. 2 that the DMV does not access the cloud platform. Thus, it cannot know who is reporting and how many videos a particular participating vehicle has reported.

3) Traceability

The traceability is an essential requirement for the reporting service to ensure that internal adversaries can be identified when a fabrication attack is mounted. In Fig. 2, it can be noticed that all entities, except the TA, cannot reveal the relationship between the utilised pseudonymous certificate and the 5G_ID identity of the sender without the knowledge of the mapping information, which is kept in the pseudonym lookup tables at the TA, which is assumed to be strongly protected.

When the authorities need to identify the sender of a particular traffic accident video file, the following steps should take place. We recall that the TA has distributed his private signing key SK_{TA} among d entities, *i.e.*, authorities, in the system at the end of the participant and official vehicle registration phase. First, the authority that initiates the tracing process should extract the pseudonymous certificate, *i.e.*, $PCert_{TA,5G\_ID,j}$, which is associated with the suspicious encrypted video file. After that, cooperation between kp authorities commences as follows according to the literature in [50]. Each authority generates a partial threshold signature $PS_i = ITHS_{\Psi i}(\Psi_i, \kappa_i, PCert_{TA,5G\_ID,j})$ on $PCert_{TA,5G\_ID,j}$ with key share Ψ_i and secret key κ_i. Then, PS_i is sent to other $(kp - 1)$ authorities for verification using $ITHV(PCert_{TA,5G\_ID,j}, PS_i)$. When kp valid signatures are gathered, any participating authority can calculate the threshold signature $TS = THS(PS_i, PCert_{TA,5G\_ID,j})$ and sends it to the TA that verifies the received threshold signature $THV(TS, PCert_{TA,5G\_ID,j})$. If the verification is successful, the TA releases the two associated hash seeds SH_1 and SH_2 in the system to revoke all the pseudonyms certificates of the vehicle 5G_ID concerned, and reveals its identity 5G_ID from the pseudonym lookup table. Finally, the TA sends the 5G_ID to the DMV to obtain the real identity of the sender's vehicle.

Thus, it is guaranteed that insufficient corrupted authorities that illegally try to reveal the identity of an innocent sender do not have the power to conduct such an action. It is guaranteed that cooperation among an approved number of different authorities including the TA should take place to do that.

B. Efficiency Analysis

In this section, we analyse the efficiency of our proposed protocol in terms of encrypting, transmitting, retrieving and decrypting a traffic accident video file. All the benchmarks in this analysis were run on an Intel Core i7-2600 3.4 *GHz* processor using crypto++ library 5.6.2 [51]. The overhead of certificates updating and the storage of pseudonymous certificates and signing keys are not considered in our discussion because they are performed annually and offline during the vehicles' inspection as explained before. We discuss the authentication overhead in terms of message signing and verification for different pseudonymous authentication methods that can be utilised in our service including the BP scheme, ECPP protocol, Hybrid scheme and the PASS scheme adopted in this paper. Furthermore, we discuss the performance of different symmetric encryption algorithms with different video file sizes and analyse the total time needed to encrypt, transmit and decrypt the reported

video file with different connection speeds that are expected in the near future in 5G enabled vehicular networks.

1) Authentication Overhead

Prior to verifying the message signature, the recipient should verify the sender's certificate. In order to do that, the recipient checks the CRL to see whether the sender's certificate is revoked. If not, the recipient proceeds with the signature verification. If successful, the message will be accepted. The verification process of the sender's certificate can be performed by the cloud and saves time on the recipient side. However, to deter the cloud from misbehaving or if it is compromised, the recipient can still randomly decide to perform this verification. Table II shows the costs of signing and verifying for the BP, ECPP, Hybrid, and PASS schemes where N_{CRL} is the size of CRL [32]. It can be noticed from the results in Table II that the certificate verification process dominates the authentication overhead. Using the group-based signature mechanism in the Hybrid scheme results in high certificate verification overhead while the PASS and BP schemes have the lowest overhead since the TA directly signs the issued pseudonymous certificates.

TABLE II – SIGNING AND VERIFICATION COSTS

	Signing cost (ms)	*Certificate verification (ms)*	*Signature verification (ms)*	*Total (ms)*
PASS	0.6	1.2	1.2	3
ECPP	0.6	14.7	1.2	16.5
Hybrid	0.6	$14.7+3.1N_{CRL}$	1.2	$16.5+3.1N_{CRL}$
BP	0.6	1.2	1.2	3

2) Cryptographic Operations and Communication Overhead

In our proposed service, the TA chooses the secure symmetric encryption/decryption *SEnc*(·) algorithm. In the following, we analyse the performance of three common block cipher algorithms that can be chosen by the TA: AES/CBC (256-bit key), Twofish/CTR (256-bit key) and Serpent/CTR (256-bit key) where their processing speeds are 455 *MB/s*, 147 *MB/s* and 65 *MB/s*, respectively. The video file size is variable and the utilised hash function is SHA-512 with a processing speed of 231 *MB/s*. The connection speed is 1.2 *Gbps* in the 5G enabled vehicular network. Finally, we used the *cpabe* toolkit [52] and MIRACL [53] library to benchmark the performance of CP-ABE and PEKS algorithms, respectively.

After capturing the video file TV_r, the sender uses *SEnc*(·) to encrypt it in *Step* 10. The time needed to perform the encryption operation $S_{PEKS} \leftarrow PEKS(PK_R, kw)$ of the keyword set *kw* in *Step* 11 is approximately 36.52 *ms*. The encryption process $ABE_C \leftarrow ABE.Enc(PK_{ABE}, S_{key}, Policy)$ in *Step* 12 takes approximately 62 *ms* with *Policy* = {'police vehicle' OR 'ambulance' OR 'traffic law enforcement' OR 'traffic authority'}, which includes four attributes. Using SHA-512, the sender generates the hash value of the following items $\{Enc_C \| S_{PEKS} \| ABE_C \| h(U)\}$ and sign it in *Step* 13, where the signature generation takes approximately 0.6 *ms*. Fig. 3 shows the time overhead for encrypting and signing the captured video file of each examined algorithm.

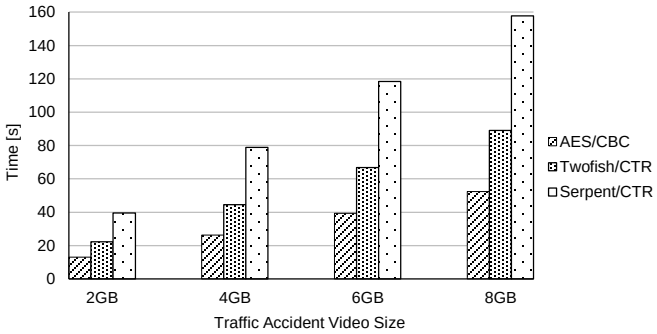

Fig. 3. Encryption/Signing Time Overhead

Assuming an instant notification from the cloud platform to the nearest official vehicle, the retrieving process proceeds as follows. The recipient verifies the received message by performing the certificate verification in *Step* 16 and the sender's signature verification in *Step* 17. From Table II, the certificate verification using the PASS scheme takes 1.2 *ms* while the message signature verification takes 1.2 *ms*. The recipient uses *ABE.Dec*(·) to extract the symmetric decryption key S_{key} in *Step* 18, which takes approximately 18 *ms*. Then, it uses *SDec*(·) to decrypt the received encrypted video file in *Step* 19. The resulted time overhead of verifying and decrypting the received video file for each examined algorithm is very similar to the results in Fig. 3. This is due to the fact of using symmetric cryptography and the similar performance of *ABE.Dec*(·) and *ABE.Enc*(·) functions.

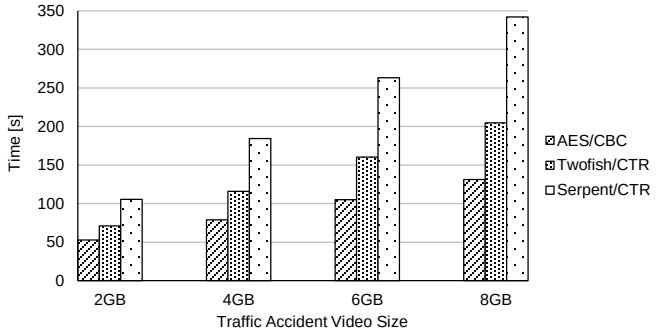

Fig. 4. Overall Time Overhead

Finally, the estimated time to upload the encrypted traffic accident video file to the cloud or retrieve it from the cloud using 5G communication links is T_{comm} = 13.3*s* as explained in Section VI-A. Note that we assume the same set of parameters for the recipient, *i.e.*, its velocity is 100 *km/h* and the 5G link connection speed is 1.2 *Gbps*. Fig. 4 shows the overall time overhead from acquiring the captured traffic accident video file at the sender and receiving it at the recipient using our proposed protocol in Fig 2. The total time overhead includes the time needed to encrypt, sign, transmit, verify and decrypt the reported video file.

To summarise, our proposed protocol can guarantee to report the traffic accident to the nearest designated official vehicle in less than one minute when the video file is 2GB and AES/CBC is utilised. Here, we assume that the sender is encrypting the traffic accident video file while capturing it, *i.e.*, the encryption of the captured accident video will finish

immediately with a very little delay. Fig. 4 shows that our proposed real-time reporting service presents an excellent replacement of the offline methods that are currently used for the same purpose, *e.g.*, [54], which could take days. Moreover, it is anticipated that the connection speeds for the 5G enabled vehicles will be higher than 1.2 *Gbps* as 1 *Tbps* speed has been achieved recently for stationary wireless connection [55]. To elaborate more on the effect of the expected connection speeds on this service, Fig. 5 shows the total time overhead of the proposed service with different connection speeds for the 5G cellular network with a 2GB accident video file.

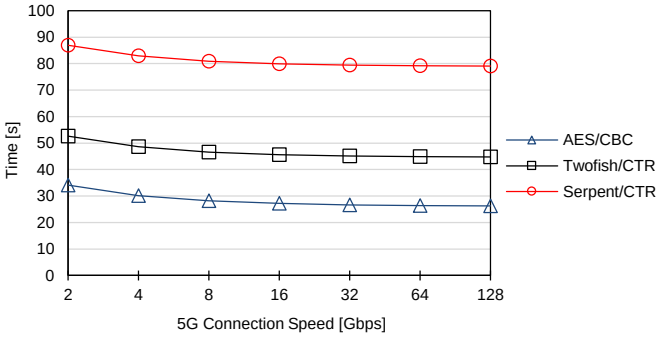

Fig. 5. Overall Time Overhead with Different 5G Connection Speeds

It can be seen in Fig. 5 that the cryptographic operations overhead will be the main bottleneck for this service. Therefore, there are two possible solutions to improve the overall time overhead in Fig. 5. First, it is recommended to equip the vehicles with improved hardware to accelerate the cryptographic operations. Secondly, the cryptographic operations and the proposed protocol can be also improved to enhance the performance of the proposed service. With the arrival of 5G cellular networks, we expect the proposed service to have a noticeable impact on the society and promote timely response toward traffic accidents to reduce the number of causalities and potentially save more lives on the roads.

VII. Conclusion

In this paper, we proposed a novel system model for a 5G enabled vehicular network that facilitates a secure and privacy-aware video reporting service. The ultimate objective of this service is to instantly report the videos of traffic accidents to the nearest official vehicle in order to improve safety on the roads. The proposed reporting service protocol is designed to take advantage of the expected features of 5G cellular networks in terms of high-speed connections, low latency and reduced cost. Moreover, it provides strong security and privacy against attacks that attempt to track a participating vehicle's identity or reveal the contents of the reported accident video. The privacy of the participants is protected against internal and external adversaries that might compromise small cells, D2D communications relays or the cloud platform. Furthermore, the proposed protocol guarantees that insufficient corrupted authorities cannot reveal the identity of a participating vehicle and cooperation among an approved number of different authorities should take place to do that. Finally, we analysed the efficiency of the proposed service and showed that a traffic accident video can be reported in a secure and privacy-preserving way in less than one minute to the official vehicles to guarantee a quick response toward traffic accidents.

References

[1] "FP7 European Project 317669 METIS (Mobile and Wireless Communications Enablers for the Twenty-Twenty Information Society)," 2012. [Online]. Available: http://www.metis2020.com/. [Accessed 06 May 2015].
[2] "FP7 European Project 318555 5G NOW (5th Generation Non-Orthogonal Waveforms for Asynchronous Signalling)," 2012. [Online]. Available: http://www.5gnow.eu/. [Accessed 06 05 2015].
[3] "5G-Infrastructure Public-Private Partnership," 2013. [Online]. Available: http://5g-ppp.eu/. [Accessed 06 May 2015].
[4] X. Shen, "Device-to-Device Communication in 5G Cellular Networks," IEEE Network, vol. 29, no. 2, pp. 2-3, 2015.
[5] Cisco, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020," Cisco, USA, Feb 2016.
[6] E. Belyaev, A. Vinel, A. Surak, M. Gabbouj, M. Jonsson and K. Egiazarian, "Robust vehicle-to-infrastructure video transmission for road surveillance applications," *IEEE Trans. Veh. Technol.*, vol. 64, no. 7, pp. 2991-3003, Sept. 2014.
[7] M. Eiza, Q. Ni, T. Owens and G. Min, "Investigation of routing reliability of vehicular ad hoc networks," *EURASIP J. Wireless Commun Netw.*, vol. 2013, no. 1, pp. 1-15, 2013.
[8] M. Eiza, T. Owens, Q. Ni and Q. Shi, "Situation-Aware QoS Routing Algorithm for Vehicular Ad hoc Networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 12, pp. 1-16, Dec 2015.
[9] A. Vinel, C. Campolo, J. Petit and Y. Koucheryavy, "Trustworthy broadcasting in IEEE 802.11 p/WAVE vehicular networks: delay analysis," *IEEE Commun. Letters*, vol. 15, no. 9, pp. 1010-1012, 2011.
[10] Z. Hameed Mir and F. Filali, "LTE and IEEE 802.11p for vehicular networking: a performance evaluation," *EURASIP J. Wireless Commun. Netw.*, vol. 2014, no. 89, 2014.
[11] A. Vinel, "3GPP LTE Versus IEEE 802.11p/WAVE: Which Technology is Able to Support Cooperative Vehicular Safety Applications?," *IEEE Wireless Commun. Letters*, vol. 1, no. 2, pp. 125-128, 2012.
[12] B. Bellalta, E. Belyaev, M. Jonsson and A. Vinel, "Performance Evaluation of IEEE 802.11p-Enabled Vehicular Video Surveillance System," *IEEE Commun. Letters*, vol. 18, no. 4, pp. 708-711, 2014.
[13] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong and J. C. Zhang, "What Will 5G Be?," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065-1082, 2014.
[14] G. Horn and P. Schneider, "Towards 5G Security," in *Proc. IEEE TrustCom* 15, Helsinki, Finland, 2015.
[15] Erricson, "5G Security," Erricson White Paper, 2015.
[16] G. Mantas, N. Komninos, J. Rodriguez, E. Logota and H. Marques, "Security for 5G Communications," in *Fundamentals of 5G Mobile Networks*, John Wiley & Sons, Ltd, 2015, pp. 207-220.
[17] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20-27, 2015.
[18] M. Alam, D. Yang, J. Rodriguez and R. A. Abd-Alhameed, "Secure Device-to-Device Communication in LTE-A," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 66-73, 2014.
[19] 3GPP, "Feasible Study for Proximity Services (ProSe)," 2013.
[20] 3GPP, "Study on Architecture Enhancements to Support Proximity Services (ProSe)," 2013.
[21] M. Raya and J.-P. Hubaux, "The Security of Vehicular Ad hoc Networks," in *Proc. SASN '05*, Alexandria, VA, USA, 2005.
[22] X. Lin, X. Sun, P.-H. Ho and X. Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442-3456, 2007.
[23] A. Studer, E. Shi, F. Bai and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," in *Proc. SECON'09*, Rome, 2009.
[24] K.-A. Shim, "CPAS: An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1874-1883, 2012.

[25] P. Kamat, A. Baliga and W. Trappe, "Secure, Pseudonymous, and Auditable Communication in Vehicular Ad Hoc Networks," *J. Security and Commun. Netw.*, vol. 1, no. 3, pp. 233-244, 2008.
[26] J. Sun, C. Zhang, Y. Zhang and Y. Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," *IEEE Trans. Parallel and Distributed Sys.*, vol. 21, no. 9, pp. 1227-1239, 2010.
[27] C. T. Barba, L. U. Aguiar, M. A. Igartua, J. Parra-Arnau, D. Rebollo-Monedero, J. Forné and E. Pallarès, "A collaborative protocol for anonymous reporting in vehicular ad hoc networks," *Comput. Standards and Interfaces*, vol. 36, no. 1, p. 188–197, 2013.
[28] M. K. Reiter and A. D. Rubin, "Crowds: anonymity for Web transactions," *ACM Trans. Information and System Security*, vol. 1, no. 1, pp. 66-92, 1998.
[29] W. Hu, K. Xue, P. Hong and C. Wu, "ATCS: A Novel Anonymous and Traceable Communication Scheme for Vehicular Ad Hoc Networks," *International J. Netw. Security*, vol. 13, no. 2, pp. 71-78, 2011.
[30] V. Daza and J. D. Ferrer, "Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 4, pp. 1876-1886, 2009.
[31] B. H. Kim, K. Y. Choi, J. H. Lee and D. H. Lee, "Anonymous and traceable communication using tamper-proof device for vehicular Ad Hoc Networks," in *Proc. ICCIT*, Gyeongju, 2007.
[32] Y. Sun, R. Lu, X. Lin, X. Shen and J. Su, "An Efficient Pseudonymous Authentication Scheme With Strong Privacy Preservation for Vehicular Communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3589-3603, 2010.
[33] R. Lu, X. Lin, H. Zhu, P.-H. Ho and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. INFOCOM*, Phoenix, 2008.
[34] G. Calandriell, P. Papadimitratos, J.-P. Hubaux and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proc. VANET'07*, Montreal, 2007.
[35] D. Boneh, G. D. Crescenzo, R. Ostrovsky and G. Persiano, "Public Key Encryption with Keyword Search," in *Proc. Eurocrypt*, Switzerland, 2004.
[36] J. Baek, R. Safiavi-Naini and W. Susilo, "Public Key Encryption with Keyword Search Revisited," in *Proc. ICCSA*, Perugia, Italy, 2008.
[37] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in *IEEE Sympos. Security and Privacy*, Oakland, CA, 2007.
[38] A. Shamir, "How to Share a Secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979.
[39] W. H. Chin, Z. Fan and R. Haines, "Emerging technologies and research challenges for 5G wireless networks," *IEEE Wireless Commun.*, vol. 21, no. 1, pp. 106 - 112, 2014.
[40] T. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. Wong, J. Schulz, M. Samimi and F. Gutierrez, "Millimeter Wave Mobile Communications for 5G Cellular: It Will Work!," *IEEE Access*, vol. 1, pp. 335 - 349, 2013.
[41] H. Ishii, Y. Kishiyama and H. Takahashi, "Novel architecture for LTE-B: C-plane/U-plane split and phantom cell concept," in *Proc. GLOBECOM*, Anaheim, CA, 2012.
[42] Q. Li, H. Niu, G. Wu and R. Q. Hu, "Anchor-booster based heterogeneous networks with mmWave capable booster cells," in *Proc. GLOBOCOM*, Atlanta, GA, 2013.
[43] C.-X. Wang, F. Haider, X. Gao, X.-H. You, Y. Yang, D. Yuan, H. Aggoune, H. Haas, S. Fletcher and E. Hepsaydir, "Cellular architecture and key technologies for 5G wireless communication networks," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 122-130, Feb 2014.
[44] F. Haider, H. Wang, H. Haas, D. Yuan, H. Wang, X. Gao, X.-H. You and E. Hepsaydir, "Spectral efficiency analysis of mobile Femtocell based cellular systems," in *Proc. ICCT*, Jinan, 2011.
[45] M. Tehrani, M. Uysal and H. Yanikomeroglu, "Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 86-92, 2014.
[46] M. Eiza and Q. Ni, "An evolving graph-based reliable routing scheme for VANETs," *IEEE Trans. Veh. Technol.*, vol. 62, no. 4, pp. 1493-1504, May 2013.
[47] J. Darroch, R. Dunphy and F. Flint, "Virtual Video Transcoding in the Cloud," 2014. [Online]. Available: http://www.intel.com/content/www/us/en/communications/virtual-transcoding-cloud-artesyn-dell-paper.html. [Accessed 11 Nov 2015].
[48] M. Riley, K. Akkaya and K. Fong, "A survey of authentication schemes for vehicular ad hoc networks," *Security and Commun. Netw.*, vol. 4, no. 10, p. 1137–1152, 2011.
[49] A. Scroxton, "Samsung claims 5G speed record," ComputerWeekely, 15 Octoer 2014. [Online]. Available: http://www.computerweekly.com/news/2240232676/Samsung-claims-5G-speed-record. [Accessed 26 June 2015].
[50] J. Baek and Y. Zheng, "Identity-based threshold signature scheme from the bilinear pairings," in *Proc. ITCC*, Las Vegas, 2004.
[51] W. Dai, "Crypto++® Library 5.6.2 - a free C++ class library of cryptographic schemes," Crypto++, 20 Feb 2013. [Online]. Available: http://www.cryptopp.com/. [Accessed 27 June 2015].
[52] J. Bethencourt, A. Sahai and B. Waters, "Advanced Crypto Software Collection - Ciphertext-Policy Attribute-Based Encryption," 24 Mar 2011. [Online]. Available: http://hms.isi.jhu.edu/acsc/cpabe/index.html. [Accessed 15 Nov 2015].
[53] CertiVox UK Ltd., "Multiprecision Integer and Rational Arithmetic Cryptographic Library – the MIRACL Crypto SDK," 10 Nov 2011. [Online]. Available: https://www.certivox.com/miracl. [Accessed 14 Nov 2015].
[54] Police Witness, "PoliceWitness.com: Report an incident," PoliceWitness, 05 January 2014. [Online]. Available: http://www.policewitness.com/report-incident/. [Accessed 26 May 2015].
[55] BBC News, "5G researchers manage record connection speed - BBC News," BBC, 25 Feb 2015. [Online]. Available: http://www.bbc.co.uk/news/technology-31622297. [Accessed 28 June 2015].

Mahmoud Hashem Eiza (M'15) received the M.Sc. and Ph.D. degrees in electronic and computer engineering from Brunel University London, London, U.K., in 2010 and 2015, respectively. He is a Research Assistant with the Department of Computer Science, Liverpool John Moores University, Liverpool, U.K. His research mainly focuses on computer, communication, and network security, with specific interests in QoS and wireless network security and privacy in vehicular networks, smart grids, cloud computing, and Internet of things.

Qiang Ni (SM'08) received the B.Sc., M.Sc., and Ph.D. degrees from Huazhong University of Science and Technology, Wuhan, China, all in engineering, in 1993, 1996, and 1999, respectively. He is a Professor of Communications and Networking with the School of Computing and Communications, Lancaster University, Lancaster, U.K. Prior to that, he led the Intelligent Wireless Communication Networking Group at Brunel University London, London, U.K. He has published more than 120 papers in his areas of interest. His main research interests include wireless communications and networking. Dr. Ni was an IEEE 802.11 Wireless Standard Working Group Voting Member and a contributor to the IEEE wireless standards.

Qi Shi received the Ph.D. degree in computing from Dalian University of Technology, Dalian, China, in 1989. He is a Professor of computer security and the Director of the PROTECT Research Center with the Department of Computer Science, Liverpool John Moores University, Liverpool, U.K. He has published nearly 200 papers in his areas of interest and managed a number of research projects with funding from various sources, such as the Engineering and Physical Sciences Research Council and the European Union. His research is centered on network security and privacy, including system-of-systems security, intrusion and denial-of-service detection, cryptography, and sensor network and cloud security.