This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2697949, IEEE Internet of Things Journal

Secure, LTE-based V2X Service

Kazi J. Ahmed, and Myung J. Lee

***Abstract*—Internet of Things (IoT) is the reality of a new and powerful ubiquitous technology. One of its main driving forces is the 3rd Generation Partnership Project (3GPP) Long Term Evolution (LTE), seeking to encompass all the applications of IoT. With this trend, 3GPP has finally made the Release 14 for LTE-based Vehicle to Everything (V2X) service. In this proposed work, we evaluated the new LTE-based V2X architecture in regards to V2X message delivery and security requirements. We showed that a proper resource allocation and reference point (channel) selection could accommodate all types of V2X message deliveries. However, focusing more on security, we deemed that LTE-based V2X security falls short of meeting adequate security requirements, especially to well preserve the privacy. Hence, we proposed a privacy preserving security for LTE-based V2X service. Considering the privacy as the top security requirement, we seamlessly integrate our security scheme with the specified LTE security architecture. Our scheme is scalable while fulfilling basic wireless message security requirements. We also provide the security and performance analysis to show the robustness and effectiveness of our proposed schemes.**

***Index Terms*—Security, privacy, trust, scalability, Intelligent Transportation System (ITS), Long Term Evolution (LTE), vehicle-to-everything (V2X) services.**

I. Introduction

IN an effort to connect everything with everything else, the Internet of Things (IoT) becomes a reality of a new and powerful ubiquitous technology. IoT is not only interconnecting devices, vehicles, buildings, cities etc. but in an efficient and smart way. Connected vehicle is one of the important focus areas of IoT, where the communication between vehicle to vehicle (V2V), vehicle to infrastructure (V2I), vehicle to pedestrian (V2P), and vehicle to Network (V2N) are provided. This vehicle to everything (V2X) communication service promises to improve the efficiency and the safety of today's transportation system by regular-interval and event-triggered message broadcasts. IEEE 802.11p and IEEE 1609 standards for Wireless Access for Vehicular Environments (WAVE) have already defined an architecture and standardized set of services and interfaces that collectively enable this requirement. In the meantime, the 3rd Generation Partnership Project (3GPP) have completed its Release 14, exclusively for Long Term Evolution (LTE)-based V2X service [1-4]. On the other hand, regulatory bodies of motor vehicles throughout the globe are planning to enforce V2X technology soon. For example, United States Department of Transportation (USDOT) is pursuing to put V2V technology on 100% of the new car production by 2021 [5]. In the beginning phase, Intelligent Transportation System (ITS) of USDOT considered IEEE WAVE technology for connected vehicle. However, it was not realized lack of infrastructure. Researchers also provided critical analyses between IEEE WAVE and LTE for this emerging technology [6-10]. To them LTE seems to be better, owing to its infrastructure, tremendous capacity increase in the near future (5G), and added direct device-to-device (D2D) communication service. Their analyses were encouraging and expedited 3GPP to finally complete and publish its Release 14 for V2X service in 2016. In this proposed work, we will critically analyze LTE-based V2X service, especially how it could accommodate different types of V2X message deliveries and fulfill the apropos security requirements.

The main motivations for connected vehicle are to reduce casualty, provide better safety and create efficient traffic movement on the street. This can be done by exchanging messages between vehicles and infrastructures. To this regard, National Highway Traffic Safety Administration (NHTSA) of USDOT makes a list of messages for V2X service. Among them are basic safety message (BSM), Intersection Movement Assist (IMA), Left Turn Assist (LTA) etc. [11]. The European Telecommunications Standards Institute (ETSI) has also defined two types of messages: cooperative awareness messages (CAMs) and decentralized environmental notification messages (DENMs) [12]. In a nutshell, all V2X messages could be broadly classified as 1) periodic and 2) event-triggered short messages [9].

Security is essential for any communication, and connected vehicle (V2X) service is no exception. The most important security requirement for V2X service is the privacy protection [5,19,20,22,23]. The message should not offer any inkling of the identity of the sender, since most V2X messages include location information. However, the traceability has to be enforced so that no one may create havoc on the street playing false information [23]. Therefore, non-repudiation has to be enacted as well [22]. Moreover, security has to be such that a single V2X User Entity or a group should not able to plot (frame) against any other for false information that it did not commit [19].

In this work, we attempt to evaluate LTE-based V2X service regarding its message delivery and specified security. We also provide some suggestive solutions for its short comings, particularly in the preservation of privacy. However, due to limited space, our work focus more on security. Since NHTSA of USDOT and Department of Motor Vehicle (DMV) are already heavily engaged in managing the vehicles, we feel their authoritative presence is important especially to enforce the security [5,7]. Therefore, our security solution deems LTE as the service provider and the Transportation Authority (TA) is the overseer of the safety and security of V2X service.

The organization of the paper is as follows. Section II provides the LTE-based V2X architecture, and section III evaluates the architecture with respect to the message delivery and security requirements. Section IV presents our proposed security scheme. Section V puts forth the security analysis of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2697949, IEEE Internet of Things Journal

the proposed work, while section VI provides a performance analysis, and finally section VII concludes the paper.

II. LTE-BASED V2X ARCHITECTURE

Before we evaluate the LTE-based V2X service, we briefly describe its current architecture (Release 14). Also for the convenience of presentation, V2X User Entity (UE) will be denoted as V-UE unless otherwise stated.

According to Rel. 14, there are two modes of operation for V2X messages [3]. These are 1) over LTE-Uu (radio interface between eNodeB and UE), 2) over PC5 (direct interface between two UEs) reference points, as shown in Fig. 1. Over the LTE-Uu reference point, V-UE can either transmit/receive unicast V2X messages or transmit unicast but receive broadcast message through Multimedia Broadcast Multicast Service (MBMS) delivery. On the other hand, over PC5 reference point, V-UE can communicate V2X messages using Sidelink channel. This is generally perform in the form of one-to-many communications, e.g. sending messages to members within a group.

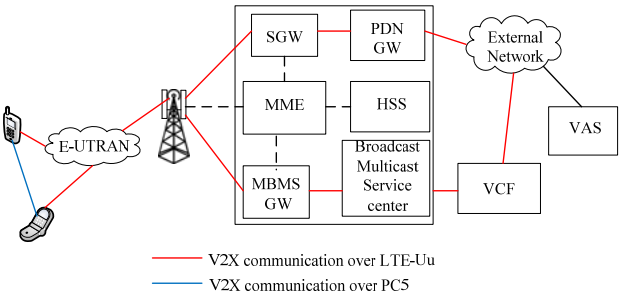

Fig. 1. LTE-based V2X communication channels.

Two additional modules are specified by 3GPP for subscription, provision and delivery of the V2X service: V2X Control Function (VCF), V2X Application Server (VAS). The VCF module provides the authorization and revocation of V2X service. During the authorization, VCF provisions V2X service specific parameters to a V-UE after mutual authentication and security key generation [13]. On the other hand, Mobile Management Entity (MME) downloads subscription information related to V2X from HSS. MME also provides indication to the Evolved Universal Mobile Telecommunications System Terrestrial Radio Access Network (E-UTRAN) about the V-UE authorization status on V2X use. Moreover, VAS module is responsible for distribution of V2X messages to different target areas. First, it receives messages from V-UEs, then summarizes the information to generate and broadcast specific V2X messages to specific locations using MBMS.

Resource over LTE-Uu reference point is provisioned using the *scheduled resource allocation*. This provisioning could be either dynamic or semi-persistent. The semi-persistent one is used for faster access of the resource in periodic fashion without requesting it repeatedly from the eNodeB (eNB) [4]. Communication over PC5 reference point uses Sidelink channel, and the resource grant may be provided by *scheduled resource allocation* (mode 1), or *autonomous resource allocation* (mode 2). In mode 2, a V-UE can acquire resource block (RB) by sensing or random selection from a pool of resources defined by eNB. To attain proper Quality of Service (QoS), V-UE uses a parameter named, Proximity Service (ProSe) Per-Packet Priority (PPPP). V-UE provides priority information reflecting this PPPP to the eNB during resource request procedure [3]. However, PPPP is not viable for mode 2 autonomous resource allocation in Rel.14. For unicast communication between V-UEs, a Source and a Destination Layer-2 IDs are used, whereas a Layer-2 Group ID is used for one-to-many communication. In addition, to ensure that a V-UE cannot be tracked or identified beyond a certain short time-period, the source Layer-2 ID can be changed over time [3]. Further, 3GPP also specified stationary infrastructure Road Side Unit (RSU), but only regarded as an implementation option. This RSU could be a combination of a V-UE with the V2X application logic or comprise an eNB, a collocated Local Gateway (L-GW), and a VAS.

III. LTE-BASED V2X MESSAGE DELIVERY AND SECURITY

Serving different V2X messages requires intelligent utilization of specified LTE-based V2X resources. Moreover, localized V2X data exchange should avoid the use of infrastructure nodes to reduce message latency [9]. Depending on the message periodicity, priority and the size of the target area, we categorized V2X messages into four classes. *First*, for periodic status message (m_1) of V-UEs such as speed, direction, location, semi-persistent resource allocation over LTE-Uu reference point is used. This m_1 message is not strictly time critical (<300ms). V-UEs first sent m_1 to VAS in unicast fashion, VAS then combines the information coming from many V-UEs. Finally, VAS broadcasts the summary message through MBMS delivery to proper target areas. *Second*, localized, time critical (<100ms), event-triggered messages (m_2) such as Critical Event Warning (CEW), Intersection Movement Assist (IMA), Left Turn Assist (LTA) etc. are provided over Sidelink using mode 2 autonomous resource allocation. Here V-UEs sense or randomly select RBs from the designated resource pool defined by eNB. This message has local preference and is communicated through direct message exchange among V-UEs or by RSUs. Moreover, this message is not necessarily periodic and occurs only at specific time and place. *Third*, global event-triggered message (m_3) such as lane closure, road construction, etc. can be allocated over LTE-Uu using dynamic resource scheduling. This message needs to be reached widely; therefore, VAS can broadcast this to a larger target region. This message does not need to maintain strict time delay (<300ms) and tight periodicity. *Fourth*, to assist smooth movement of emergency vehicles such as ambulance, fire truck, etc. scheduled semi-persistent resource allocation (SRA) over Sidelink channel is utilized. This localized periodic message (m_4) has local significance and needs to be sent in regular interval for a specific amount of time.

We consider end-to-end (e2e) delay in dealing with four message classes. High priority m_2 and m_4 messages with 100 *ms* while low priority m_1 and m_3 messages with 300 *ms* target. Note

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2697949, IEEE Internet of Things Journal

however that in each group of priority, each class of message is handled with different resource allocation method. Further, the first three message types (m_1, m_2, and m_3) can be accommodated using the current 3GPP specification. But the proposed resource allocation for m_4 is not specified in 3GPP Rel. 14 for V2X communication. However, SRA over Sidelink is specified in 3GPP Rel. 12 for Device-to-Device (D2D) direct discovery (type 2b) procedure. This resource allocation is requested from eNB through dedicated RRC signaling by Radio Resource Control (RRC) connected UE. Message m_4 can utilize this resource allocation procedure (SRA) without bringing forth any additional change to LTE protocols. Again, for out of coverage case, V-UE can use preconfigured values for accessing resource using the PC5 reference point.

Moreover, all these messages require no acknowledgement; hence, the number of collisions need to be reduced especially for emergency message communication. Collision may happen when V-UEs use RBs from common resource pool of PC5 channel for high priority messages (m_2, m_4). In case of resource allocation for a new m_4 message, the V-UE needs to request SRA to eNB. Upon receipt of this request, eNB selects new RBs for the requesting V-UE not to overlap with RBs allocated already to other m_4 messages. Therefore, no collision among m_4 messages. Further, eNB attaches control information blocks preceding the data blocks. Hence, other messages (m_2) can avoid collision from m_4 by sensing based on Schedule Assignment (SA) and decoding [6]. In case of m_2, the assignment of RBs from shared resource pool is performed solely and randomly by V-UEs, not by eNB. As a result the probability of collision between m_2 messages is high. Nevertheless, substantial researches have been done already to reduce the effect of collision in shared resource access [24-26]. For instance, the methods proposed in [24-25] make use of codes to increase the probability of successful transmission while sending same packet multiple times. On the other hand, [26] employs Self-Organizing TDMA (STDMA) where an additional setup phase is required before the actual assignment of RBs.

As privacy is imperative for V2X service, message has to be exchanged anonymously. However, non-repudiation, traceability, non-frame-ability are also required at the same time. 3GPP already makes a prerequisite that user specific Layer-2 and IP level ID need to be changed for anonymity. For communication between V-UE and VAS over LTE-Uu, either shared-secret keys or generation of symmetric keys by Diffie-Hellman Key Exchange (DHKE) can be used. It might also be done by either SSL or TLS session creation, even though the session establishment entails additional latency. But symmetric key does not provide anonymity nor does it provide non-repudiation.

For one-to-many V2X communication through Sidelink channel, 3GPP specified to use a group security key, derived from shared secret [21]. For stronger security, session keys can be generated from shared secret and distributed by the group member initiating the communications. However, rapid change of group members in V2X context can limit its viability. Many authors also proposed different security protocols over Sidelink channel using DHKE [14-16]. Their protocols can support integrity, authenticity, non-repudiation, as well as detection of malicious nodes. Some also proposed random encryption key pre-distribution scheme to select keys from common large pool of keys [17]. Others used physical layer features to establish security keys [18]. Nevertheless, all the proposed security schemes including that of 3GPP use symmetric key algorithm [13]. In one-to-many communication, symmetric key can hold the anonymity, but it cannot provide the non-repudiation.

To remedy this security dilemma, we provide a suggestive proposition for V2X security scheme that fulfills all the above mentioned security requirements. Our work assumes that TA oversees security aspect of the V2X service. It makes sure that everyone follows according to the proposed scheme and resolves any dispute regarding fraudulent messages. Our proposed scheme is also light weight and provides scalability.

IV. Proposed V2X Security Scheme

Our proposed work assumes Transport Authority (TA) as the control and management entity of V2X service, whereas LTE is only the communication service provider. Moreover, TA is considered the trusty and cannot be compromised. To provide adequate scalability, whole region (e.g., whole USA) is divided into security domains (e.g., states) and each domain has its different level of authorities and members. TA resides at the top followed by Vehicle Pseudonym Distributors (VPDs). The V-UEs, VASs and RSUs reside at the lowest level as a member. VPDs are agents of TA which are distributed throughout the domain and considered as trusty as TA. In addition to provide pseudonym seeds (to explain later), VPD assists V-UE to smoothly transfer security keys from one domain to another. This helps V-UE continue its secure V2X service in the new domain. As V-UEs are by default connected to internet through LTE network, they can easily access TA, VPD as well as VCF and VAS. Moreover, our proposed work does not consider RSU and VAS trusty. The proposed V2X security structure is depicted in Fig. 2 and the detail is described in the following paragraphs.

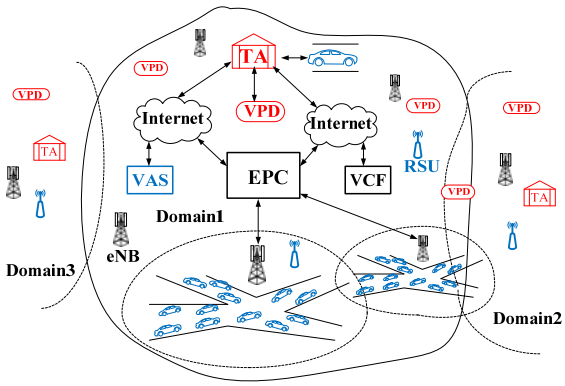

Fig. 2. Proposed security structure for V2X services

A. Key Distribution and Management

To provide privacy protection to a V-UE, two sets of security keys, namely, long-term and short-term keys are created.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2697949, IEEE Internet of Things Journal

Long-term keys are used to contact authorities, for instance, to request pseudonym seeds from VPD, while short-term keys are used to exchange V2X messages. However, these keys need to be distributed securely and, must be managed properly with no scalability issues. The key distribution and management of our security scheme follows four phases described below.

1) Domain Initialization

At first each security domain TA sets up its master secret $M_{TA} = \langle x_1, x_2 \rangle$, where $1 \leq x_i \leq p-2$ $(i = 1,2)$ where p is a large prime number. Then it creates the domain parameters $Par_{TA} = \langle p, g, y_1, y_2, \ddot{H}, H, h \rangle$, where g is the primitive root of Z_p^* which is a prime residue class group of modulo p, $y_1 = g^{x_1}$, $y_2 = g^{x_2}$. $\ddot{H}$ is a collision resistant hash, $H: H_{in} = \{0,1\}^* \rightarrow H_{out} = \{0,1\}^k \in Z_p^* \setminus \{p\text{-}1\}$, but $\notin Z_{p-1}^*$ and h is another optional hash, where $h: h_{in} = \{0,1\}^* \rightarrow h_{out} = \{0,1\}^k \in Z_p^*$ according to [19]. Here $P_{TA} = \langle y_1, y_2 \rangle$, is the public keys of the TA. TA also creates for each VPD two sets of keys, long term keys $\langle Ls_{VPD}, Lp_{VPD} \rangle$ and short-term keys $\langle Ss_{VPD}, Sp_{VPD} \rangle$ from VPD's ID and its master secret. The definitions and notations related to different keys are provided in Table 1.

TABLE 1
NOTATION OF SECURITY SYMBOLS AND KEYS

Notation	Description
$\boldsymbol{Ls_X = \ddot{H}(ID_X, r_X) \in Z_p^*}$	Long-term private key for entity *X*
$\boldsymbol{ID_X}$	Actual ID for entity *X*
$\boldsymbol{r_X}$	Random number for entity *X*
$\boldsymbol{Lp_X = g^{Ls_X} \in Z_p^*}$	Long-term public key for entity *X*
$\boldsymbol{Ss_X = (2Sp_X x_1 + x_2)\ H(Sp_X)\ mod(p-1)}$	Short-term private key for VPD or RSU
$\boldsymbol{Sp_X = ID_X}$	Short-term public key for VPD or RSU
$\boldsymbol{E_{ns}(m; k)}$.	Symmetrical encryption with key *k*
$\boldsymbol{E_n(m; s)}$.	Asymmetrical encryption with key *s*
$\boldsymbol{Sm_{A-B}}$	Symmetric key between *A* and *B*
$\boldsymbol{SD_V{}^j = A_V{}^j \parallel t_V{}^j \parallel r_{VSD}{}^j \parallel sig(h(A_V{}^j \parallel t_V{}^j); Ss_{VPD})}$	*j*-th pseudonym seed for V-UE *V*
$\boldsymbol{A_V{}^j = Lp_V{}^{r_{VSD}{}^j}}$	*A* parameter of *j*-th seed for V-UE *V*
$\boldsymbol{r_{VSD}{}^j}$	*j*-th seed random number for V-UE *V*
$\boldsymbol{t_V{}^j}$	*j*-th seed expiration time for V-UE *V*
$\boldsymbol{sig(h(A_V{}^j \parallel t_V{}^j); Ss_{VPD})}$	Signature on *j*-th seed for V-UE *V*
$\boldsymbol{Sp_V{}^j = \langle Sp_{V_1}{}^j \parallel Sp_{V_2}{}^j \rangle}$	*j*-th short-term public key for V
$\boldsymbol{Sp_{V_1}{}^j = g^{B_{V_1}{}^j}}$	First part of *j*-th public key
$\boldsymbol{Sp_{V_2}{}^j = g^{B_{V_2}{}^j} = A_V{}^j}$.	Second part of *j*-th public key
$\boldsymbol{B_{V_1}{}^j = r_V{}^j Ls_V}$;	First *B* parameter for *j*-th key
$\boldsymbol{r_V{}^j}$	Random number for *j*-th key
$\boldsymbol{B_{V_2}{}^j = r_{VSD}{}^j Ls_V}$	Second *B* parameter for *j*-th key
$\boldsymbol{Ss_V{}^j = (B_{V_1}{}^j + B_{V_2}{}^j)\ H(Sp_{V_1}{}^j \oplus Sp_{V_2}{}^j) mod(p-1)}$	*j*-th short-term private key for V

The VPDs at the boundaries get keys from all neighboring TAs. TA will also provide the domain parameter Par_{TA} and public keys of VPD $\langle Lp_{VPD}, Sp_{VPD} \rangle$ to the VCF of its domain. At this time, RSUs and VASs also get their keys from its domain TA as $\langle Ss_{RSU}, Sp_{RSU} \rangle$ and $\langle Ss_{VAS}, Sp_{VAS} \rangle$ respectively.

2) V2X Domain Registration

To get V2X services, at first each vehicle has to register at its TA. At this time the TA will create only the long-term keys $\langle Ls_V, Lp_V \rangle$ (not the short-term keys which preserve privacy to be explained later) and the signature $sig(Lp_V; M_{TA})$, and load these into the temper resistant On Board Unit (OBU) of the vehicle. Signature and other security processes of our security structure is presented in Table 2.

3) V2X Service Registration

After V2X domain registration, a V-UE sends Registration Request (Req.) message to VCF, including a DHKE key part (g^a) as shown in Fig. 3. VCF in reply sends ID Req. message to the V-UE with the other key part (g^b) of DHKE. At this moment, both V-UE and VCF can create common symmetric key $k_s = (g^a)^b = (g^b)^a = g^{ab}$. Now, V-UE sends its International Mobile Subscriber Identity (IMSI) ID encrypted by the symmetric key k_s, $E_{ns}(IMSI_V; k_s)$ to VCF. To get Authentication Vector (AV) for this V-UE, VCF sends V2X Authentication (Auth.) data Req. to HSS. HSS creates AV including the integrity Key (IK") and Confidentiality Key (CK") from IDs of both V-UE and VCF. Now HSS responds back to VCF using V2X Auth. data Response (Res.). Then, VCF sends V2X Auth. Req. to V-UE including a part of the AV (AUTH, RAND). From the provided part of AV, V-UE creates same IK", CK", RES and sends V2X Auth. Res. including RES. VCF compares HSS provided RES and V-UE provided RES, and if they match, V-UE is considered authentic. After this mutual authentication, VCF sends Registration Res. including $\mathrm{Par_{TA}}$, $\mathrm{Lp_{VPD}}$, $\mathrm{Sp_{VPD}}$, and V2X related parameters. Finally, V-UE submits its long-term public key $\mathrm{Lp_V}$ and the signature of TA $\mathrm{sig(Lp_V; M_{TA})}$ to VCF encrypted with the CK" as $\mathrm{E_{ns}([Lp_V \parallel sig(Lp_V; M_{TA})]; CK")}$. VCF on the other hand, verifies $\mathrm{Lp_V}$ by the provided signature of the TA, $\mathrm{ver(Lp_V; P_{TA})}$ as defined in Table 2, and maps the public key with the other information of the V-UE (vehicle) for later use as $\mathrm{map_{VCF}(Lp_V \Rightarrow IMSI, \ldots)}$.

TABLE 2
DEFINITION OF DIFFERENT SECURITY PROCESSES

Security processes	Definition
$\boldsymbol{sig(m; M_{TA}) = (2mx_1 + x_2)H(m) mod(p-1)}$	Signature of TA
$\boldsymbol{ver(m; P_{TA})}$: $(y_1{}^{2m} y_2)^{H(m)} = g^{sig(m; M_{TA})}$	Verification of signature of TA
$\boldsymbol{sig(m; Ss_X)}$: $(g^{r_1}, r_1{}^{-1}(\ddot{H}(m) - (2g^r + 1)(Ss_X)))$ $. mod(p-1) = (\rho, \sigma)$	Signature of VPD, RSU, VAS
$\boldsymbol{ver(m; Sp_X)}$: $(((y_1)^{2Sp_X} y_2)^{2\rho+1})^{H(Sp_X)} \rho^{\sigma} = g^{\ddot{H}(m)}$	Verification of signature of VPD, RSU, VAS
$\boldsymbol{E_n(m; Sp_X)}$: $(g^r, m \oplus h((y_1)^{2Sp_X} y_2)^{rH(Sp_X)}) = (U, V)$	Asymmetric encryption for VPD
$\boldsymbol{D_n(E_n(m; Sp_X))}$: $(V \oplus h(U)^{Ss_X})$	Asymmetric decryption by VPD or RSU
$\boldsymbol{sig(m; Ss_V)}$: $(g^{r_2}, r_2{}^{-1}(\ddot{H}(m) - (g^{r_2} + 1)(Ss_V)))$ $mod(p-1) = (\rho_1, \sigma_1)$	Signature of V-UE V
$\boldsymbol{ver(m; Sp_V)}$: $((Sp_{V_1} Sp_{V_2})^{\rho_1+1})^{H(Sp_{V_1} \oplus Sp_{V_2})} \rho_1{}^{\sigma_1} = g^{\ddot{H}(m)}$	Verification of signature of V

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2697949, IEEE Internet of Things Journal

4) V-UE Pseudonym Generation

After V2X registration, each V-UE needs to create short-term (pseudonym) keys in order to exchange V2X message securely. First, the V-UE sends Pseudonym (Pseu.) Seed Req. to VPD, encrypted by the public key of VPD Sp_{VPD} acquired at the time of registration as $E_n([ID_{req} \parallel Lp_V \parallel P_{TA} \parallel sig(Lp_V; M_{TA})]; Sp_{VPD})$. Here ID_{req} is a request ID to distinguish the request message. VPD on the other hand, decrypts the message using D_n, verifies the signature of TA, $ver(Lp_V; P_{TA})$ (Table 2), and creates a symmetric key $Sm_{V-VPD} = (Lp_{VPD})^{Ls_V} = [(g^{Ls_{VPD}})^{Ls_V} = (g^{Ls_V})^{Ls_{VPD}} = (Lp_V)^{Ls_{VPD}}$.

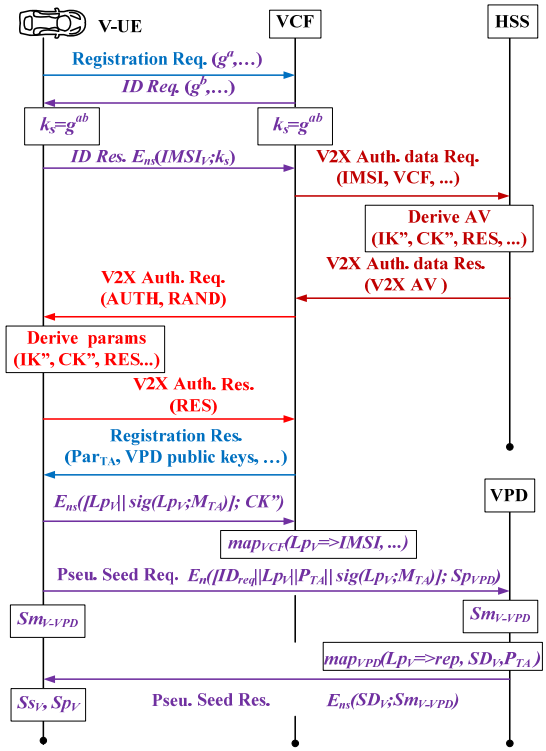

Fig. 3. V2X Service Registration and Pseudonym Generation

Next, VPD generates the pseudonym seed (SD_V), encrypts it by the symmetric key, $E_{ns}(SD_V; Sm_{V-VPD})$ and sends it to the requested V-UE (Pseu. Seed Res.). This provided seed will include signed expiration time so that the generated pseudonym will be valid only for a specific period. The definition and related parameters of seed are given in Table 1. To provide scalability in key management and to speed up (light weight) the verification process, we provide expiration time rather than Certificate Revocation List (CRL) according to [20]. On the other hand V-UE creates the same symmetric key Sm_{V-VPD} from $\langle Lp_{VPD}, Ls_V \rangle$ and decrypts the received (Pseu. Seed Res.) seed from VPD. The V-UE now creates its pseudonym keys (short-term keys) Ss_V and $Sp_V = \langle Sp_{V_1}, Sp_{V_2} \rangle$ from the given seed for secure V2X message exchange. The first part of public key Sp_{V_1} is created by the V-UE itself, whereas the second part Sp_{V_2} is provided by the VPD (Table 1). In the mean time VPD maps the given seed SD_V, a revocation parameter *rep* and others with the public key of the V-UE as $map_{VPD}(Lp_V \Rightarrow rep, SD_V, P_{TA})$. This given seed and the created short-term keys from it works only for a specific time period. When the pseudonym expires, V-UE immediately renews it through the Pseu. Seed Req. and Pseu. Seed. Res. procedure. Whenever VPD is requested for a pseudonym seed, it checks the revocation status of the V-UE from its domain TA. VPD provides the pseudonym seed only if the revocation status of the V-UE is OK. Moreover, VPD removes stored information of the V-UE ($map_{VPD}(Lp_V \Rightarrow rep, SD_V, P_{TA})$) once the SD_V is expired and creates and stores whenever a new request is completed. Consequently, the size of the stored information does not grow constantly as opposed to CRL approach.

B. Secure V2X Message Exchange

In this subsection we explain how the four types of messages mentioned in section III can be securely exchanged. Rather than using encryption, which requires group keys, V-UE and RSUs send signed plain text V2X messages. These messages assist only to attain safety and the efficiency of the traffic movement and do not produce confidential information. To preserve the privacy, each V-UE frequently changes, as often as every message, its short-term keys $\langle {Ss_V}^j, {Sp_V}^j \rangle$ (Table 1). V-UE also requires to change its Layer-2 ID and IP address as well for anonymity in MAC and Network layer. To prevent replay attack, all types of messages include time stamp as m_i = (message || t_{stamp}).

As we discussed earlier that the m_1 is sent from V-UE to VAS in unicast fashion, however with the following format.
$(m_1 \parallel Sp_{VPD} \parallel Sp_V \parallel t_V \parallel sig(h(A_V, t_V); Ss_{VPD}) \parallel sig(h(m_1); Ss_V))$
When VAS receives the message, it first performs $ver(h(A_V \parallel t_V); Sp_{VPD})$ using t_V, $Sp_V (= \langle Sp_{V_1} \parallel A_V \rangle)$ and Sp_{VPD}, then it checks validity of $ver(h(m_1); Sp_V)$ (Table 2). The first verification assures that the pseudonym key is valid and current, whereas the second one guarantees that the message comes from a legitimate V-UE. When VAS broadcasts the combined summary in response, the message is delivered through MBMS to a target area. This MBMS is entirely controlled by Evolved Packet Core (EPC) of LTE and therefore, this broadcast does not need security signing. The m_2 , which is localized event-triggered message, may be sent either by V-UE or RSU. If the message is sent by a V-UE, the format is the same as that of the m_1, however the receivers are other V-UEs. The verification process of this message follows the same procedure. If this is sent by RSU, then the format is $(m_2 \parallel Sp_{RSU} \parallel sig(h(m_2); Ss_{RSU}))$ and the verification requires to check $ver(h(m_2); Sp_{RSU})$. To assist this verification process, a list of public keys Sp_{RSU_i} of RSUs are provided by VCF to a V-UE at the time of its registration. The global triggered message m_3 is sent by V-UEs to VAS, and the signing and verification process is the same as that of the m_1 message. Localized periodic message m_4, is sent mostly by the emergency vehicle V_E-UE with the format, $(m_4 \parallel Sp_E \parallel sig(h(m_4); Ss_{V_E}))$. The verification is done by performing $ver(h(m_4); Sp_{V_E})$ and again a list of public keys $Sp_{V_{E_i}}$ of emergency vehicles V_E-UEs are procured at the time of registration.

If two V-UEs V_X and V_Y want to communicate with each

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2697949, IEEE Internet of Things Journal

other in unicast fashion, they can do so by encrypting the message. For this, a common symmetric key needs to be created. This is done by using the short-term public keys Sp_V, found from previous message exchange as $Sm_{V_{X-V_Y}} = Sp_{V_{X_2}}{}^{B_{V_{Y_2}}} = A_{V_X}{}^{B_{V_{Y_2}}} = \left(g^{B_{V_{X_2}}}\right)^{B_{V_{Y_2}}} = \left(g^{B_{V_{Y_2}}}\right)^{B_{V_{X_2}}} = A_{V_Y}{}^{B_{V_{X_2}}} = Sp_{V_{Y_2}}{}^{B_{V_{X_2}}}$. Refer to Table 1 for parameters used here. The message format for this unicast is $\left(ID_m \parallel Sp_{V_Y} \parallel E_{ns}(m;\ Sm_{V_{X-V_Y}})\right)$ where ID_m is the message ID to recognize it as an encrypted V2X unicast message. The receiver V_Y finds its symmetric keys from the attached Sp_{V_Y} in the message.

C. Revocation and Cross Domain Procedure

A V-UE or a group of V-UEs may spread false information such as lane closure and road construction ahead, to gain some unfair advantage or even to send false emergency alert to panic others. If a certain V-UE finds that its received message is fraudulent, it may start the revocation process by reporting the message of the rogue V-UE V_r to VPD. Reporting message also follows the same security measures as those of V2X messages. Before accepting any report, VPD verifies the reporter properly, i.e. it verifies that the reporter's short-term keys are current ($ver(h(A_V \parallel t_V); Sp_{VPD})$) and it is a registered legitimate one ($ver(h(m_1); Sp_V)$). After successful verification, VPD increments the corresponding revocation parameter *rep* ($map_{VPD}(Lp_V \Rightarrow rep, SD_V, P_{TA})$) by one. However, this value is increased only if the report comes from disjoint events and for different short-term keys $Sp_{V_r}{}^i$ ($rep \Rightarrow value^i, event^i, Sp_V{}^i$). Once *rep* attains a certain threshold value, VPD retrieves the public key Lp_{V_r} from its *map* and provides it to its TA. To recover the public key, VPD first retrieves A_{V_r} from Sp_{V_r} $(= \langle Sp_{V_{r_1}} \parallel A_{V_r} \rangle)$ found in the rogue message and finds the corresponding SD_{V_r}, and then from SD_{V_r}, finds Lp_{V_r} (Table 1). The threshold value of *rep* can range from two to some higher value depending on how harsh or relaxed the revocation implementation is. TA on the other hand, sends the public key (Lp_V) of the corresponding rogue V-UE to VCF. Finally, VCF searches for the ID of this V-UE from its record ($map_{VCF}(Lp_V \Rightarrow IMSI, \ldots)$) and revokes it from V2X service. TA also notifies all its VPDs about the revocation so that they stop providing any more pseudonym seed (SD_V).

When a V-UE moves to a new security domain, it will immediately request a new pseudonym seed from the nearest VPD it comes across. VPD always checks the revocation status of V-UE from the TA before it provides a new seed. If the TA is not in the security domain of this VPD, it requests its TA to verify the revocation status to the V-UE's TA (P_{TA} found in the request message) on its behalf.

V. Security Analysis

In this section we analyze our proposed security protocol with respect to the common security attacks.

A. Privacy Attack

To attack privacy of other V-UEs, an attacker could capture many broadcast packets and try to link messages to the same V-UE to unfold, for instance, its location information. However it is not possible in our security scheme since V-UE will frequently change its short-term key to sign the V2X messages. Moreover, if an attacker compromises VPD, it only gets the long-term public key and associated materials that do not provide V-UE's real identity. Finally, an attacker cannot get actual IMSI from listening to the V2X Service Registration message exchange since it is encrypted by the symmetric key $E_{ns}(IMSI_V; k_s)$.

B. Traceability

A rogue V-UE may hide its trace under the identity of others. The attacker V-UE *X* may capture Sp_{V_Y} and $sig(h(A_Y \parallel t_Y); Ss_{VPD})$ from broadcast message of some V-UE *Y* and attach it to its own fraud message to pretend of being V-UE *Y*. However when the message receivers use Sp_{V_Y} to perform $ver\left(h(m_X); Sp_{V_X}\right)$, verification fails. Further, the V-UE *X* may forge the signature of VPD, $sig\left(h(A_{V_X} \parallel t_X); Ss_{VPD'}\right)$ by itself and use a corresponding fake public key Sp_{V_X} $(= \langle Sp_{V_{X_1}} \parallel A_{V_X} \rangle)$, which has no trace of the V-UE. But when any other V-UE uses real public key of VPDSp_{VPD} to verify this false signature $ver(h(A_X \parallel t_X); Sp_{VPD'})$, again it fails. The message can pass verification only when the legitimate V-UE uses true Sp_V. Likewise, a legitimate V-UE can always be traced by the authority as explained in revocation section.

C. Frame-ability

As the revocation process needs to have a threshold number of reports to be in effect, some V-UEs might attempt to get other V-UE revoked. These V-UEs together may send the same reports multiple times to revoke a V-UE. However, without being disjoint events, they are counted only as one report. Moreover, a V-UE or two may send a report and wait for the same short-term key to be seen to place another report. But multiple reports for same short-term key are also considered as one report.

D. Attack from compromised user

An attacker can use a compromised V-UE to broadcast false message for its own benefit. However the revocation process kicks in immediately and the compromised V-UE will lose its grant for V2X service. In addition, the attacker may use this V-UE to produce false pseudonym requests to VPD. However, to retrieve the provided seed from the encrypted message, attacker has to find the long-term private key Ls_V of the V-UE resided inside the OBU. If the attacker attempts to break the temper resistant OBU, it will end up destroying all security materials instantly.

E. Attack from compromised VPD

A compromised VPD can impersonate a V-UE by creating pseudonym from the long-term public key Lp_V, stored in its *map*. However the *B* parameters, $B_{V_1} = r_V Ls_V$, $B_{V_2} = r_{VSD} Ls_V$ of short-term private key Ss_V are generated from the long-term private key (Table 1). Hence to impersonate a V-UE, VPD has to collude with the trustworthy TA which is not possible.

F. Replay Attack

In the proposed scheme, message format *m* (= message $\parallel$ t_{stamp}) also includes the time stamp and is protected by the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2697949, IEEE Internet of Things Journal

sender signature $sig(h(m); Ss_V)$. To successfully replay the same message, the attacker not only need to change the time stamp and also the corresponding signature.

G. Key escrow problem

In our proposed scheme, even though TA creates and hence knows the long-term key pair of a V-UE, these keys will be used only for communicating with the authority. The V2X message communication is secure only by short-term key pair Ss_V and Sp_V..These keys are solely generated by the V-UE itself from the provided pseudonym seeds; hence, the key escrow problem does not exist in this proposed security scheme.

VI. Performance Analysis

Even though security is the top requirement for V2X services, the performance is also important specially for the practicality of the implementation. In the following, we will analyze the performance of our protocol for the effectiveness of practicality.

A. Overhead Cost

To calculate the total overhead cost of our security scheme, we assume 256 bit-size of short-term and 512 bit-size of long-term keys for a V-UE. On the other hand, for special entities TA, RSU and VPD, we assume to use 512 bit keys for better security.

To calculate the overhead cost of V2X message sent by a V-UE, we use the format presented in section IV subsection B. $\left(m \parallel Sp_{VPD} \parallel Sp_V \parallel t_V \parallel sig(h(A_V, t_V); Ss_{VPD}) \parallel sig(h(m); Ss_V)\right)$ This message could be m_1,m_2 or m_3. In this message, the public key of VPD takes 512 bits, public key of V-UE needs 256 bits, expiration time (t_V) and message timestamp (m = message || t_{stamp}) require 2×4 bytes (Unix Timestamp), signature of V-UE occupies 2×256 bits and signature of VPD occupies 2×512 bits (Table 2), making a total amount of $(512 + 256 + 2 \times 4 \times 8 + 2 \times 256 + 2 \times 512) \div 8 = 296$ bytes. Message sent by RSUs or emergency vehicles V_E-UE has this format $\left(m \parallel Sp_X \parallel sig(h(m); Ss_X)\right)$ and the security overhead occupies $(512 + 4 \times 8 + 2 \times 512) \div 8 = 196$ bytes. This message could be m_2 by RSU or m_4 by V_E-UE. Note here that the overhead V-UE message is higher than that of RSU and of V_E-UE because of the contradicting security requirement for V-UE: privacy and traceability. According to current LTE structure, each RB is composed of 7 symbols and 12 subcarriers. Again for a bandwidth of 20 MHz, a single LTE Slot carries 100 RBs according to standard. Hence one Subframe which is two times the size of one Slot would carry 200 RBs. Now, for a symbol of 6 bits (64-QAM) each RB is $(6 \times 7 \times 12) \div 8 = 63$ bytes long. Hence the security overhead of our proposed scheme occupies around 5 RBs for message sent by V-UE (m_1,m_2,m_3) and 4 RBs for message from RSU (m_2) or V_E-UE (m_4).

B. End-to-End Delay

To calculate the e2e delay of different messages, we measure the processing time (PT) of different security modules using Java eclipse. The Java codes run on a Lenovo computer, with 5 Computer Cores, 2C + 3G, 2.2 GHz, 8 GB RAM, 64 bit OS and is shown in Table 3.

TABLE 3
Processing Time For Different Security Modules

Algorithm	PT (256 bits)	PT (512 bits)
$\boldsymbol{sig(Lp_V; M_{TA})}$	2ms	6ms
$\boldsymbol{ver(Lp_V; M_{TA})}$	3 ms	8ms
$\boldsymbol{E_n(m;\ Sp_{VPD})}$	4ms	9ms
$\boldsymbol{D_n(E_n(m;\ Sp_{VPD}))}$	2ms	6ms
$\boldsymbol{E_n(SD_V;\ Sm_{V-VPD})}$	<1ms	<1ms
$\boldsymbol{D_n(E_n(SD_V;\ Sm_{V-VPD}))}$	<1 ms	<1ms
$\boldsymbol{sig(h(A_V, t_V); Ss_{VPD})}$	2ms	6ms
$\boldsymbol{ver(h(A_V, t_V); Sp_{VPD})}$	3ms	8ms
$\boldsymbol{sig(h(m); Ss_V)}$	2ms	6ms
$\boldsymbol{ver(h(m); Sp_V)}$	3ms	8ms

Table 4 shows different parameters used to calculate e2e delay for all types of V2X messages. Note here that the bulk of the message generation process (GPT) time is coming from the signature, whereas message reception process time (RPT) from the verification. Hence, the main contribution to e2e delay comes GPT, RPT, and RBs procurement time (RBT). In case of m_1 and m_3, an additional time is required for processing of messages and procurement of RBs by VAS (VPT).

TABLE 4
e2e Delay Calculation for Different V2X Messages

Message	By	GPT	RPT	RBT	VPT
m_1	V-UE	2 ms	9 ms	Yes	yes
m_2	V-UE	2 ms	9 ms	Yes	no
m_2	RSU	6 ms	6 ms	Yes	no
m_3	V-UE	2 ms	9 ms	Yes	Yes
m_4	V_E-UE	6 ms	6 ms	Yes	No

The e2e delay of messages m_1 and m_3 depends mostly on the LTE-Uu link (source to destination) delay. The current theoretical LTE-Uu link delay is less than 10 ms [9]. However, practical LTE-Uu delay (including resource scheduling) can be shown less than 50 *ms* using the delay analysis presented in [27-28]. Hence, the total e2e delay for m_1 and m_3, from V-UE through LTE-Uu to VAS and from VAS to target area through MBMS, including security overhead could be made comfortably within 300 *ms*. For m_4, SRA from shared resource pool is allocated through eNB; therefore, e2e delay depends on the semi-persistence period (SPP). According to 3GPP, current SPP could be made as low as 10 *ms*. As a result, the e2e delay for m_4 including security overhead can be made well within the critical time 100 *ms*. In case of m_2, the effective e2e delay depends on the probability of successful transmission. In low density situation, multiple transmission of the same packet within a resource pool period (RPP) could increase the probability of success close to 1[25]. Note that the localized event-triggered message m_2, such as CEW, IMA, LTA, is generated by few users at a particular time and place. Moreover, according to 3GPP specification RPP could be made as low as 40 subframes (40 *ms*); hence, the total e2e delay of m_2 could also be achieved within the critical time 100 *ms*.

C. Scalability

In our protocol, each TA is responsible for storing registration and revocation information of V2X entities only of its own domain. VPD holds information related to current

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2697949, IEEE Internet of Things Journal

pseudonym seeds of requested V-UEs. To find a rogue V-UE VPD needs to search through all the current seed-keys, $Sp_V{}^j = \langle Sp_{V_1}, Sp_{V_2} \rangle, j = 1\ to\ m$ of all the *N* V-UEs. Here the searching time for VPD is O(n) where $n = m*N$, whereas if it is done by a single TA covering the whole region, the required time would be 5000 folds (50 states and 100 VPD in each state). Again, VPD removes the *map* and the corresponding info once the pseudonym seed is expired. This makes the list of provided seeds relatively constant over time unlike the ever increasing CRL. Moreover, the authority does not have to distribute CRL every time an entity gets revoked. In that case it would consume a lot of bandwidth and is not very scalable (1% rate of revoked vehicles of $5.2x10^6$ will be $52x10^3$ vehicles and equal size of CRL). Again, the receiver of the V2X massage does not need to go through time consuming CRL for verification process.

VII. Conclusion

We have proposed a security architecture of LTE-based V2X communication. We seek to evaluate the LTE-based V2X architecture specified in 3GPP Release 14 regarding message delivery and security requirements. We incorporate all types of V2X messages with the specified resource allocation and reference points. We showed that an efficient resource allocation and proper reference point selection can successfully provision any type of V2X message service. We also evaluated its security based on the V2X security requirements and found out that the privacy is not fully secured. Hence we proposed a practical solution, not only to provide privacy, but also to fulfill basic security requirements of wireless message exchange. We seamlessly integrate our security scheme with the specified LTE architecture. Finally, we put forth security and performance analysis to show the robustness and effectiveness of our protocol. In future we would extend our security architecture for other applications like vehicle-to- smart grid.

References

[1] 3GPP, TS 36.331 V14.0.0, Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification.

[2] 3GPP, TS 36.321 V14.0.0, Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification.

[3] 3GPP, TS 23.285 V14.0.0, Architecture enhancements for V2X services.

[4] C. Hoymann *et al*., "LTE release 14 outlook," in *IEEE Communications Magazine*, vol. 54, no. 6, pp. 44-49, June 2016.

[5] "20 questions about Connected Vehicles", last visited Feb. 2017, http://www.its.dot.gov/cv_basics/cv_basics_20qs.htm.

[6] S. h. Sun, J. l. Hu, Y. Peng, X. m. Pan, L. Zhao and J. y. Fang, "Support for vehicle-to-everything services based on LTE," in *IEEE Wireless Communications*, vol. 23, no. 3, pp. 4-8, June 2016.

[7] H. Seo, K. D. Lee, S. Yasukawa, Y. Peng and P. Sartori, "LTE evolution for vehicle-to-everything services," in *IEEE Communications Magazine*, vol. 54, no. 6, pp. 22-28, June 2016.

[8] Vinel, A., "3GPP LTE Versus IEEE 802.11p/WAVE: Which Technology is Able to Support Cooperative Vehicular Safety Applications?" in *Wireless Communications Letters, IEEE* , vol.1, no.2, pp.125-128, April 2012.

[9] Araniti, G.; Campolo, C.; Condoluci, M.; Iera, A.; Molinaro, A., "LTE for vehicular networking: a survey," in *IEEE Communications Magazine,* , vol.51, no.5, pp.148-157, May 2013.

[10] Hameed Mir and Filali,"LTE and IEEE 802.11p for vehicular networking: a performance evaluation," *EURASIP Journal on Wireless Communications and Networking 2014.*

[11] http://www.safercar.gov/staticfiles/safercar/v2v/V2V_Fact_Sheet_101414_v2a.pdf, August 20, 2014.

[12] ETSI EN 302 665, Intelligent Transport Systems (ITS); Communications Architecture,Sept. 2010.

[13] 3GPP, TS 33.833 V1.8.0, Study on security issues to support Proximity Services.

[14] A. Zhang, J. Chen, R. Hu, and Y. Qian, "SeDS: Secure data sharing strategy for D2D communication in LTE-Advanced networks," in *IEEE Transactions on Vehicular Technology,* vol. PP, no. 99, pp. 1, March, 2015.

[15] W. Shen, W. Hong, X Cao, Bo Yin; D. Shila, and Y. Cheng, "Secure key establishment for Device-to-Device communications," in *IEEE Global Communications Conference (GLOBECOM)*, pp. 36-340, December 2014.

[16] Abd-Elrahman, E.; Ibn-khedher, H.; Afifi, H.; Toukabri, T., "Fast group discovery and non-repudiation in D2D communications using IBE," in *Wireless Communications and Mobile Computing Conference (IWCMC)*, 2015 International , vol., no., pp.616-621, 24-28 Aug. 2015.

[17] L. Goratti, G. Steri, K. Gomez, and G. Baldini, "Connectivity and security in a D2D communication protocol for public safety applications," in *11th International Symposium on Wireless Communications Systems (ISWCS)*, pp. 548- 552, August. 2014.

[18] W. Xi, X. Li, C. Qian, J. Han, S. Tang, J. Zhao, and K. Zhao, "KEEP: Fast secret key extraction protocol for D2D communication," in *IEEE 22nd International Symposium of Quality of Service (IWQoS)*, pp. 350- 359, May 2014.

[19] Ahmed, Kazi J.; Lee, Myung J.; Li, Jie, "Layered scalable WAVE security for VANET," in *IEEE Military Communications Conference, MILCOM 2015 - 2015* , vol., no., pp.1566-1571, 26-28 Oct. 2015.

[20] André Weimerskirch," V2V Communication Security: A Privacy Preserving Design for 300 Million Vehicles," in *Workshop on Cryptographic Hardware and Embedded Systems 2014 (CHES 2014)*, Sept. 2014.

[21] 3GPP, TS 23.303 V14.0.0, Proximity-based services (ProSe); Stage 2.

[22] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, A. Lioy, "Efficient and robust pseudonymous authentication in VANET" *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, pp 19-28, 2007.

[23] X. Lin, X. Sun, P. 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.

[24] E. Paolini, C. Stefanovic, G. Liva and P. Popovski, "Coded random access: applying codes on graphs to design random access protocols," in *IEEE Communication Magazine*, vol. 53, no. 6, pp. 144-150, June 2015

[25] Laurent Gallo and J´erˆome H¨arri, " Self Organizing TDMA over LTE Sidelink " Research Report RR-17-329, EURECOM, Jan. 2017

[26] L. Gallo and J. H¨arri, "Short paper: A LTE-direct broadcast mechanism for periodic vehicular safety communications," in VNC 2013, IEEE Vehicular Networking Conference (VNC), Boston, USA, December 2013, pp. 166–169.

[27] J. Fabini and T. Zseby, "The Right Time: Reducing Effective End-to-End Delay in Time-Slotted Packet-Switched Networks," in *IEEE/ACM Transactions on Networking*, vol. 24, no. 4, pp. 2251-2263, Aug. 2016.

[28] M. Laner, P. Svoboda, P. Romirer-Maierhofer, N. Nikaein, F. Ricciato and M. Rupp, "A comparison between one-way delays in operating HSPA and LTE networks," *2012 10th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*, Paderborn, Germany, 2012, pp. 286-292.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2697949, IEEE Internet of Things Journal

Mr. Kazi J. Ahmed received his B.Sc. and M.Sc. degree from Bangladesh University of Engineering and Technology (BUET) in Electrical and Electronic Engineering. He is a PhD Candidate and working towards his PhD in the City College of New York at City University of NY. He is also an adjunct faculty in the City College of New York. His research area includes IEEE WAVE-based VANET, LTE-based V2X, IoT, Vehicle-to-Grid, and their Security. He published two of his papers in IEEE WAVE-based VANET Security at UKC 2015 and at Milcom 2015. He also has publised two of his papers in Digital Signal Processing (DSP) at ICECE 2006 and at Journal of IEB 2006. Currently he is working on Secure Resource Allocation in LTE-based V2X service towards 5G Network.

Dr. Myung J. Lee (SM) received a B.S and an MS from Seoul National University in Korea and Ph.D degree from Columbia University in electrical/electronics engineering. He is currently a professor at the Dept of Electrical & Computer Engineering of City College and Graduate Center of City University of New York. He is also an adjunct professor of GIST. Dr. Lee's recent research interests include V2X, Security, IoT, mobile cloud computing, VANET, Vehicle-to-Grid applications. He published extensively in these areas including a book (Green IT: Technologies and Applications, Springer)(ed.) and more than 25 U.S and international patents. He is a technical editor for IEEE communications magazine. Dr. Lee also actively contributes to international standard organizations IEEE and ZigBee (currently the chair of IEEE 802.15.8 PAC). Dr. Lee's research group developed the first NS-2 simulator for IEEE 802.15.4, a standard NS-2 distribution widely used for wireless sensor network researches. He co-received the best paper awards at IEEE CCNC 2005 and 1st EAI conference on Smartgrid2016 and CUNY Excellence Performance Award. He is a past president of KSEA.