PAL - Privacy Augmented LTE: A Privacy-Preserving Scheme for Vehicular LTE Communication

Daniel Angermeier
Fraunhofer Research Institution AISEC
Munich, Germany
daniel.angermeier@aisec.fraunhofer.de

Alexander Kiening
Fraunhofer Research Institution AISEC
Munich, Germany
alexander.kiening@aisec.fraunhofer.de

Frederic Stumpf
Fraunhofer Research Institution AISEC
Munich, Germany
frederic.stumpf@aisec.fraunhofer.de

ABSTRACT

We propose a novel privacy-preserving scheme for LTE in vehicular communication. The main idea behind our concept is to include original equipment manufacturers (OEM) of vehicular stations in the mobile connection's life cycle. Our scheme makes use of pseudonymous identifiers and splits the identity management for communicating vehicles between mobile network operators and OEMs. We show that our scheme improves the privacy of subscribers without loss of functionality in terms of all relevant use cases for vehicular communication over LTE.

Categories and Subject Descriptors

C.2.0 [**General**]: Security and protection (e.g., firewalls); C.2.5 [**Local and Wide-Area Networks**]: Access Schemes

Keywords

Security; Privacy; LTE; V2X

1. INTRODUCTION

Upcoming *Vehicle-to-X* (V2X) communication promises safer and more efficient road traffic (see, e. g., [10, 14]). In V2X communication, vehicles exchange messages with other vehicles or infrastructure. On the one hand, this allows vehicles to broadcast safety-relevant messages, like hazardous road condition or emergency break event warnings. On the other hand, V2X communication enables the provision of services to V2X participants. Service providers can offer their services via direct communication with their users, or on the internet, using a vehicle's communication capabilities and a supporting infrastructure. While wireless communication over ETSI ITS G5 [2] constitutes the basis for V2X communication, additional mobile communication network technologies like *Long Term Evolution* (LTE) offer increased flexibility. Furthermore, the inclusion of mobile communication network technologies helps bridge the expected gap in G5 coverage especially during the introduction phase of V2X communication. However, current mobile communication network technologies enable *mobile network operators* (MNO) to track their customers. This counters the privacy-preserving measures undertaken by G5 communication, where vehicles use *pseudonyms* and a distributed *Public Key Infrastructure* (PKI) to protect the privacy of the passengers (see, e. g., [12]). While, arguably, subscribers implicitly accept this loss of privacy when signing a mobile service contract for their phone, this does not necessarily hold true for customers buying a car. Therefore, similar to the G5 approach, a privacy-preserving scheme for mobile network communication in a V2X environment is needed.

Thus, we propose a novel privacy-preserving scheme for LTE communication in vehicular networks. We especially focus on LTE since this is the most recent standard. In addition, most aspects we cover with our approach also apply to older standards like GSM and UMTS, as LTE evolved from these standards. Our scheme distributes privacy critical identifiers for subscribers among MNOs and *original equipment manufacturers* (OEM) of *Intelligent Transportation System Vehicle Stations* (IVS). The scheme preserves the privacy of *Intelligent Transportation System* (ITS) users as long as MNOs and OEMs do not cooperate maliciously. Additionally, our proposed scheme supports correct billing of ITS users without impairing privacy.

In Section 2, we discuss related work before we give a short overview of aspects of regular LTE relevant for our work in Section 3. Section 4 gives a short analysis of threats and potential attackers. Section 5 shows the use cases we consider for LTE in V2X communication. In Section 6, we highlight the requirements for a privacy-preserving scheme for LTE in V2X communication. Afterwards, we present the details of our scheme in Section 7. In Section 8, we analyze whether our scheme meets the requirements defined in Section 6. We conclude with a summary in Section 9. Finally, we list the most important abbreviations inside the glossary at the end of this document.

2. RELATED WORK

Several papers on privacy enhancement in LTE exist. However, as far as we know, none considers MNOs as potential attackers. Arapinis et al. [3] discuss new threats to user

VANET'13, June 25, 2013, Taipei, Taiwan
Copyright 2013 ACM 978-1-4503-2073-3/13/06 ...$15.00.

privacy in a 3G environment, and propose and verify protocol fixes. While their approach highlights important additional aspects of mobile telephony privacy, their attacker model, unlike ours, does not include MNOs as potential attackers. Choudhury et al. [4] introduce the *Dynamic Mobile Subscriber Identity* (DMSI), which replaces the *International Mobile Subscriber Identity* (IMSI) in the *Evolved Packet System - Authentication and Key Agreement* (EPS-AKA) protocol. By not transmitting the IMSI in plain text, they protect the privacy of subscribers against third parties sniffing on the aerial link. Furthermore, their approach also protects the privacy of subscribers against attackers eavesdropping on wired connections in the backbone of the mobile network. However, their attacker model also does not include MNOs. In all of these cases, MNOs can break the privacy of their subscribers.

Several papers on privacy protection in G5 communication exist, e. g., Papadimitratos et al. [12] describe privacy protecting measures in G5 V2X communication, where vehicles use pseudonymous certificates and a carefully designed PKI to protect the privacy of drivers. However, the requirements for G5 differ from those in LTE communication, since, e. g., billing is not required for G5. Consequently, the attacker models differ, as G5 does not rely on infrastructure entities as much as LTE does.

3. BACKGROUND INFORMATION ON LTE

In regular LTE, subscribers use their *User Equipment* (UE) to connect to the mobile network maintained by their MNO. During the life cycle of such connections, the MNO gains knowledge of several identifiers of its connected subscribers. In the following, we describe these identifiers and their purposes.

For the authentication process, the UE generally identifies itself to the MNO using the subscriber's IMSI. The IMSI uniquely identifies an LTE subscriber and is described in [7]. Using the IMSI, the MNO determines a key K_{IMSI} previously shared with the UE, where a secure element, the *Universal Integrated Circuit Card* (UICC) running the *Universal Subscriber Identity Module* (USIM) application, securely stores and handles keys and cryptographic operations. Consequently, the USIM and the MNO use this key to negotiate additional keys, securing further communication between both entities (see [9] for further information on the EPS-AKA process).

To protect the privacy of subscribers against eavesdroppers, the UE and the MNO exchange the IMSI as rarely as possible. They regularly negotiate *Globally Unique Temporary IDs* (GUTI) and use these GUTIs in place of IMSIs (see [6] for details on the usage of the GUTI).

The UE also receives a *Cell Radio Network Temporary Identifier* (C-RNTI) [8] from the cell's serving eNodeB. The C-RNTI serves as a temporary pseudonymous identifier for the UE within a cell.

The *International Mobile Station Equipment Identity* (IMEI) uniquely identifies a piece of mobile equipment, e. g., a mobile phone (not its USIM or subscriber) and is described in [7]. MNOs use IMEIs, e. g., to prevent stolen equipment from using services of the mobile network.

By sending an *Identity Request*, MNOs can retrieve identifiers from UEs, such as the IMSI or IMEI.

A cascading fallback mechanism exists in various LTE events: If no GUTI is available, the UE transmits the IMSI. If the IMSI is not available either, the UE transmits the IMEI instead.

The MNO assigns an *IP address* to each UE after joining the network. The UE uses this IP address for application related communication.

The *Mobile Subscriber Integrated Services Digital Network* (MSISDN), i.e., the phone number, uniquely identifies each subscriber. MNOs map MSISDNs to IMSIs to deliver incoming calls to UEs.

Among these identifiers, the IMSI, IMEI, and MSISDN permanently identify the subscriber or the device respectively. The IP address is either a permanent or a temporary identifier for a UE, depending on the mode of assignment: the MNO can either assign IPs statically or dynamically. The GUTI and C-RNTI serve as temporary identifiers, where the mapping to a subscriber or UE is only known to the MNO who assigned them. Thus, MNOs can link each of these permanent and temporary identifiers of their own subscribers or related devices to real identities.

4. THREATS AND POTENTIAL ATTACKERS

We consider two kinds of threats to the privacy of V2X users caused by the use of LTE in vehicular communication. On the one hand, we consider *usage privacy*, i. e., only the user and the provider of a service shall know about the usage of the service. On the other hand, we consider *location privacy*, i. e., only the owner of a UE shall be able to create location profiles of the UE's movement.

In mobile communication networks, the UE regularly sends identifying information to its associated MNO (see Section 3), which allows the MNO to deduce the UE's current position:

- The IMSI represents privacy critical information, since an attacker can link the IMSI to a subscriber identity. Even if the subscriber behind an IMSI is initially unknown to an attacker, location profiles usually show a regular path between the area where a person lives and the area where this person works. Thus, an attacker could create location profiles to connect the IMSI to a person in most cases, given enough time and regular (IMSI, location) pairs. While usage of GUTIs instead of IMSIs provides some privacy protection against third parties, the IMSI still needs to be transferred in plain text from time to time. Additionally, MNOs can nevertheless perfectly track their subscribers, since MNOs can map GUTIs to IMSIs. Therefore, knowledge of an IMSI combined with location information, like, e. g., the coverage area of a cell, threatens location privacy.

- IMEIs are unique identifiers for UEs. OEMs distribute these IMEIs bundled with associated UEs. However, in regular LTE operation, UEs's IMEIs are exclusively visible to their respective MNO. Thus, MNOs can fully track UEs using IMEIs, resulting in detailed location profiles and a violation of location privacy.

- In an LTE mobile network, mobile nodes usually receive an IP address when turned on and release this IP address when turned off. Clearly, this allows MNOs to create profiles of full trips at least by mapping IP addresses to cell memberships, violating location privacy. Furthermore, since MNOs know both sides of an

IP addressed communication, they are also capable of violating usage privacy.

- The GUTI and C-RNTI serve as temporary identifiers. Given the link to permanent identifiers, both the GUTI and the C-RNTI allow tracking of subscribers. MNOs distribute these temporary identifiers. Therefore, MNOs can use them to violate location and usage privacy of subscribers.

While the current LTE standard aims to protect location and usage privacy against third parties (see, e. g., [13]), MNOs can easily create detailed location and usage profiles of their subscribers, based on the information sent by their UEs. Therefore, we consider MNOs as highly capable attackers on the location and usage privacy of their subscribers. By contrast, we do not consider service providers as attackers on usage privacy, since we assume explicit user consent in this case.

We do not consider malicious modifications to UEs, like e. g., installing a tracking device or modifying the software of the UE, as such modifications are not caused by the use of mobile communication networks in vehicular communication itself. Thus, UEs as attackers are out of scope for our work. However, since OEMs participate in our scheme (see Section 7), we also regard OEMs as potential attackers with superior capabilities compared to third party attackers.

We do not consider collusion attacks, especially between MNOs and OEMs. Resolution of pseudonymity can be a necessary requirement for, e. g., law enforcement, making complete anonymity and untraceability an undesired property.

5. USE CASES

We consider the following use cases for LTE in vehicular communication:

5.1 Internet access

One use case we consider is Internet access by IVSs[1], e. g., to fetch traffic or weather information. Internet access does not require previous knowledge of the IVS's current location by its MNO, since the connection does not originate on the network side. Instead, the IVS connects to the mobile network actively before using a service from a service provider on the Internet. Afterwards, the IVS's IP address serves as identifier to exchange data with entities on the Internet.

5.2 Geonetworking

Geonetworking is an important concept in V2X communication. In geonetworking, a message is distributed with a defined relevance area, in which presumably the message is relevant for all receivers, e. g., traffic congestion information or hazardous road condition warnings. Cell broadcasts offer a route to IVSs in a given area when G5 communication fails (e. g., caused by the absence of V2X enabled communication partners in the surroundings of a sender). Thus, in this use case, an ITS distributes information by sending a geonetworking message to a mobile network. The network's MNO then broadcasts this information in all cells which intersect the area defined by the message.

5.3 Push Services

To realize push services, an IVS subscribes to a service. Then, the service provider uses the mobile network to send data when available. Such data might, e. g., include traffic information or changes in weather conditions.

6. REQUIREMENTS

We consider these requirements for a privacy-preserving scheme for LTE in a V2X environment:

R1 **Location privacy.** An attacker shall not be able to create a location profile of any IVS's movements.

R2 **Usage privacy.** An attacker shall not be able to create a usage profile of services used by any IVS.

R3 **Pull services.** IVSs shall be able to use mobile services that require active initialization of the connection by the IVS.

R4 **Push services.** IVSs shall be able to use services which require push functionality, i. e., active notification of subscribers by their service providers.

R5 **Reachability of IVSs via cell broadcasts.** IVSs shall be reachable via cell broadcasts. Please note that this requirement does not demand targeted reachability of single IVSs initiated by a third party, since this is not relevant for cell broadcasts.

R6 **Support of billing.** The scheme shall enable the MNO to bill subscribers for used services without impairing the privacy of subscribers.

R7 **No compromise of security by the scheme.** The scheme shall not reduce the security offered by LTE. This also includes protection against forging of identities by attackers.

R8 **Minimize changes to LTE.** The scheme shall aim to avoid changes to the LTE standard where possible.

7. DESCRIPTION OF OUR SCHEME

We introduce a novel privacy-preserving scheme for LTE in V2X communication. Our scheme encompasses several aspects to achieve improved privacy for LTE subscribers in vehicular environments, as depicted in Figure 1. As shown in Section 3, MNOs gain complete knowledge of a subscriber's identity. The idea behind our concept is to include OEMs in the mobile connection's life cycle. We realize this by separating the task of managing identities between MNOs and OEMs and splitting up the gained knowledge in a way such that neither MNOs nor OEMs have sufficient knowledge to deduce subscribers' identities, locations, or service usage.

In order to achieve that, we replace all permanent identifiers from Section 3 with pseudonyms and ensure that temporary identifiers are negotiated using pseudonyms. In our scheme, MNOs create encrypted sets of pseudonyms and hand subsets of these pseudonyms to OEMs. OEMs in turn distribute subsets of these pseudonym subsets to IVSs. IVSs share a common key with MNOs, enabling the IVSs to decrypt and use the obtained pseudonyms. Thus, MNOs can only determine communicating entities to be authentic but

[1] In this paper's context, an IVS is both an LTE UE and a G5 communication node inside a vehicle.

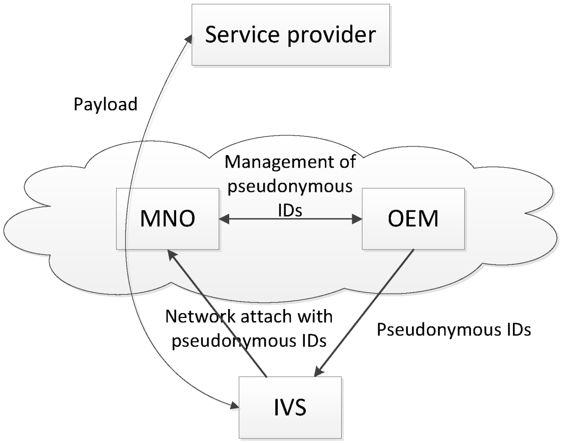
Service provider
Payload
Management of pseudonymous IDs
MNO
OEM
Network attach with pseudonymous IDs
Pseudonymous IDs
IVS

Figure 1: Our privacy-preserving scheme distributes knowledge about the IVS's identity among MNOs and OEMs. While none of the involved entities is capable of tracking the IVS, billing and service usage are still possible.

cannot derive their real identities, while OEMs have no access to the pseudonyms, keys or the mobile network infrastructure. IVSs can still use services offered by service providers by attaching to the mobile network with pseudonyms. We describe our scheme in more detail in the following subsections.

7.1 Handling of identifiers

We replace identifiers used in LTE communication with pseudonyms. This way, we prevent linkability of LTE subscriber identities to identifiers visible in LTE-based V2X communication.

Our scheme requires regular changes of pseudonymous identifiers. These changes shall occur simultaneously, since otherwise linking pseudonymous identifiers becomes an easy task. If, for example, we change the IP address, but keep all other identifiers the same, an attacker can establish a connection between the old and the new IP address by using the identifiers which remained identical. Therefore, we require regular complete reconnects using fresh pseudonyms.

For the sake of simplicity, we explain the scheme for one OEM, MNO, and IVS. We denote the encryption of plain text p, utilizing a symmetric cipher scheme using key K_{NAME}, with $\mathrm{E}_{K_{\text{NAME}}}(p)$. We denote the flow of a message m from A to B with $A \longrightarrow B : m$. Finally, $\xrightarrow{K_{\text{NAME}}}$ signifies the transmission of a message over a channel secured with a symmetric cipher scheme using key K_{NAME}.

With $\xrightarrow{K_{\text{SESSION}}}$, we denote a channel secured with a symmetric cipher scheme using a previously negotiated session key K_{SESSION}. The involved parties can, e. g., negotiate K_{SESSION} using an asymmetric cipher scheme in conjunction with a PKI, e. g., utilizing TLS [5]. A new key K_{SESSION} is negotiated for every new session.

7.1.1 IMSI

We introduce the *Pseudonymous Mobile Subscriber Identity* (PMSI), a pseudonym replacing the IMSI in most circumstances. We describe the detailed structure of a PMSI at the end of this section (7.1.1). The creation, distribution and use of PMSIs encompasses the following aspects:

Initial Setup.

The OEM creates a secret key K_{IVS} during the manufacturing process. The OEM shares this key in a secure environment with the IVS and stores the relation between this key and the IVS's USIM's IMSI. This shared secret key enables the OEM and the IVS to communicate confidentially.

$$\text{OEM} \longrightarrow \text{IVS} : K_{\text{IVS}}$$

Furthermore, the OEM owns the key pair A_{pub} and A_{priv}, where A_{pub} serves as the OEM's public key and A_{priv} as the OEM's private key in an asymmetric cipher scheme. This key pair later helps establish a secure connection between the IVS and the OEM. The OEM sends A_{pub} to the IVS in the aforementioned secure environment.

$$\text{OEM} \longrightarrow \text{IVS} : A_{\text{pub}}$$

PMSI Generation.

The MNO generates PMSIs for later deployment to IVSs and distributes all necessary information to the OEM, as also depicted in Figure 2 in the box labeled "PMSI Generation". In the following, we explain the PMSI generation in detail:

1. The MNO creates n unique PMSI and secret key K_{PMSI} pairs $\mathbf{p}_i$,
$$\mathbf{p}_i = (\text{PMSI}_i, K_{\text{PMSI}_i}),$$
where $\text{PMSI}_i \neq \text{PMSI}_j$ for all $i \neq j$ and n is a sufficiently large number, depending on the number of the MNO's subscribers and the pseudonym change frequency. The set $\mathcal{P}_{\text{MNO}}$ of all these pairs $\mathbf{p}_i$,
$$\mathcal{P}_{\text{MNO}} = \bigcup_{i=1}^{n} \{\mathbf{p}_i\},$$
constitutes the MNO's *PMSI pool*. The secret key K_{PMSI} later helps secure communication between the MNO and an IVS using the according PMSI as pseudonym. Since $\mathcal{P}_{\text{MNO}}$ is created centrally by the MNO, collisions between PMSIs are avoided.

2. The MNO creates a secret key K_{PERIOD}. Then, the MNO encrypts each $\mathbf{p}_i \in \mathcal{P}_{\text{MNO}}$ separately, utilizing a symmetric cipher scheme (e. g., AES [11]) using the key K_{PERIOD}. Finally, the OEM creates pairs of the following structure:
$$\mathbf{e}_i = (\text{PLMN}, \mathrm{E}_{K_{\text{PERIOD}}}(\mathbf{p}_i)),$$
resulting in the element-wise partially encrypted PMSI pool $\mathcal{E}_{\text{MNO}}$:
$$\mathcal{E}_{\text{MNO}} = \bigcup_{i=1}^{n} \{\mathbf{e}_i\}.$$
The MNO later shares K_{PERIOD} exclusively with its subscribers. Thus, only the MNO's subscribers can read the PMSI pairs $\mathbf{p}_i$. The validity of K_{PERIOD} is limited to a billing period to enable the reuse of PMSIs. The prepended *Public Land Mobile Network* (PLMN) serves as identifier to allow associating the encrypted PMSIs with their originating MNO.

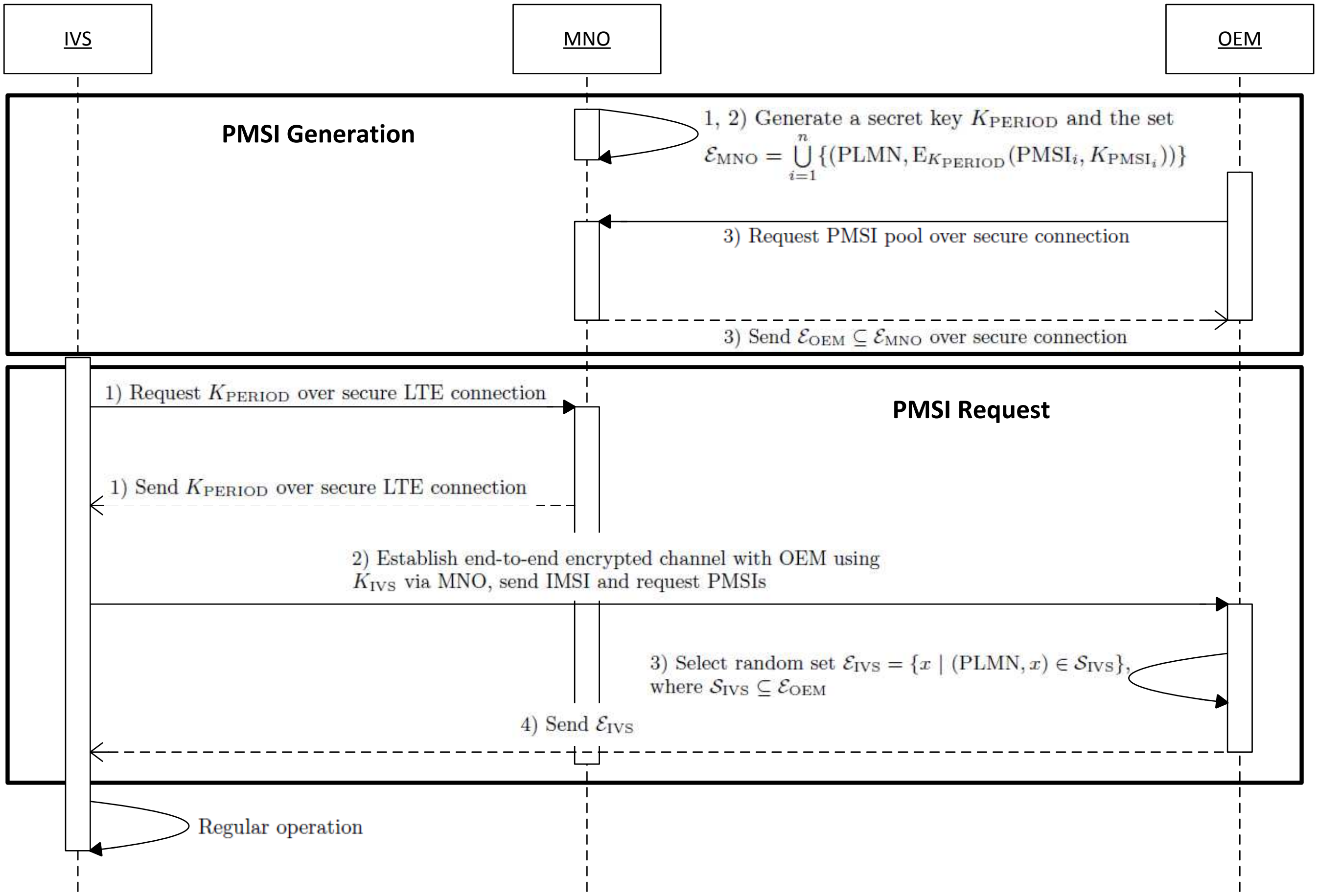
IVS
MNO
OEM
PMSI Generation
1, 2) Generate a secret key K_{PERIOD} and the set $\mathcal{E}_{\text{MNO}} = \bigcup_{i=1}^{n} \{(\text{PLMN}, \text{E}_{K_{\text{PERIOD}}}(\text{PMSI}_i, K_{\text{PMSI}_i}))\}$
3) Request PMSI pool over secure connection
3) Send $\mathcal{E}_{\text{OEM}} \subseteq \mathcal{E}_{\text{MNO}}$ over secure connection
PMSI Request
1) Request K_{PERIOD} over secure LTE connection
1) Send K_{PERIOD} over secure LTE connection
2) Establish end-to-end encrypted channel with OEM using K_{IVS} via MNO, send IMSI and request PMSIs
3) Select random set $\mathcal{E}_{\text{IVS}} = \{x \mid (\text{PLMN}, x) \in \mathcal{S}_{\text{IVS}}\}$, where $\mathcal{S}_{\text{IVS}} \subseteq \mathcal{E}_{\text{OEM}}$
4) Send $\mathcal{E}_{\text{IVS}}$
Regular operation

Figure 2: A simplified depiction of the PMSI generation and request processes as described in Section 7.1.1 between an IVS and its related MNO and OEM.

3. The OEM establishes a secure connection to the MNO. The OEM then requests PMSIs and the MNO transmits a subset

$$\mathcal{E}_{\text{OEM}} \subseteq \mathcal{E}_{\text{MNO}}$$

of the aforementioned element-wise partially encrypted PMSI pool $\mathcal{E}_{\text{MNO}}$ to the OEM and stores the relation between $\mathcal{E}_{\text{OEM}}$ and the OEM. This set $\mathcal{E}_{\text{OEM}}$ comprises the OEM's current *PMSI pool* :

$$\text{MNO} \xrightarrow{K_{\text{SESSION}}} \text{OEM} : \mathcal{E}_{\text{OEM}}$$

PMSI Request.

IVSs require new PMSIs each billing period or if they run out of valid PMSIs. Regular PMSI requests, as depicted in Figure 2 in the box labeled "PMSI Request", consist of the following steps:

1. The IVS establishes a regular secure LTE connection to the MNO. Using the IMSI and the related preshared key K_{IMSI}, the IVS and the MNO derive cryptographic material, including a temporary key K_{TEMP}. The MNO transmits the secret key K_{PERIOD} to the IVS. Note that this transmission's confidentiality is protected by regular LTE security mechanisms. The USIM stores K_{PERIOD} in its secure key storage and does not reveal it to the IVS.

$$\text{MNO} \xrightarrow{K_{\text{TEMP}}} \text{USIM} : K_{\text{PERIOD}}$$

2. The IVS establishes a secure connection to the OEM via the aforementioned secure LTE connection to the MNO. To initialize the connection, the IVS encrypts its USIM's IMSI with an asymmetric cipher scheme using the OEM's public key A_{pub}. The IVS sends this encrypted IMSI to the OEM.

$$\text{IVS} \longrightarrow \text{OEM} : \text{E}^{\text{asym}}_{A_{\text{pub}}}(\text{IMSI}),$$

where $\text{E}^{\text{asym}}_{A_{\text{NAME}}}(p)$ denotes the encryption of plain text p, utilizing an asymmetric cipher scheme using key A_{NAME}. The OEM decrypts $\text{E}^{\text{asym}}_{A_{\text{pub}}}(\text{IMSI})$ using its private key A_{priv}. Then, the OEM maps the received IMSI to K_{IVS}. A symmetric cipher scheme using key K_{IVS} secures all further communication between the IVS and the OEM. This protects the confidentiality of all exchanged messages between the IVS and the OEM against third parties, including the MNO.

3. The OEM picks a random subset of previously unused elements from its PMSI pool

$$\mathcal{S}_{\text{IVS}} \subseteq \mathcal{E}_{\text{OEM}},$$

where the PLMN part of each $\mathbf{e}_i \in \mathcal{S}_{\text{IVS}}$ matches the IMSI's PLMN part. The OEM stores the relation between $\mathcal{S}_{\text{IVS}}$ and the IVS's USIM's IMSI for billing and other purposes. To save bandwidth in the next step, the OEM removes all PLMN parts from all $\mathbf{e}_i \in \mathcal{S}_{\text{IVS}}$, resulting in $\mathcal{E}_{\text{IVS}}$.

$$\mathcal{E}_{\text{IVS}} = \{x \mid (\text{PLMN}, x) \in \mathcal{S}_{\text{IVS}}\}$$

4. The OEM sends $\mathcal{E}_{\text{IVS}}$ to the IVS via the connection secured with K_{IVS} and marks the elements in $\mathcal{S}_{\text{IVS}}$ as used.

$$\text{OEM} \xrightarrow{K_{\text{IVS}}} \text{IVS} : \mathcal{E}_{\text{IVS}}$$

Regular Operation.

For regular operation, the IVS uses regularly changing PMSIs instead of its IMSI:

1. The IVS selects an unused $\text{E}_{K_{\text{PERIOD}}}(\mathbf{p}_i) \in \mathcal{E}_{\text{IVS}}$, marks the selected element as used and sends the encrypted $\mathbf{p}_i$ to the USIM:

$$\text{IVS} \longrightarrow \text{USIM} : \text{E}_{K_{\text{PERIOD}}}(\mathbf{p}_i).$$

2. The IVS's USIM decrypts the received encrypted PMSI pair $\text{E}_{K_{\text{PERIOD}}}(\mathbf{p}_i)$ using K_{PERIOD} and stores the extracted $\mathbf{p}_i$, containing PMSI_i and the related secret key K_{PMSI_i}, in its secure storage.

3. The USIM uses this fresh PMSI_i (and related secret key K_{PMSI_i}) when negotiating a new GUTI with the MNO.

The IVS changes PMSIs regularly. The interval of changes represents a tradeoff: shorter intervals improve the privacy of ITS users, but also increase memory and communication bandwidth requirements for the storage and transmission of pseudonymous identifiers. Additionally, the total number of unique pseudonymous identifiers limits the number of possible changes within the validity period of these identifiers. IVSs should change their PMSIs as often as feasible to protect the privacy of ITS users.

Billing.

For billing, the MNO uses the OEM to charge subscribers for the MNO's services:

1. The MNO sends aggregated billing information for each $\mathbf{e}_i \in \mathcal{E}_{\text{OEM}}$ within the OEM's PMSI pool to the OEM, using a connection secured with key K_{SESSION}, established via, e. g., TLS.

2. The OEM aggregates this information for each IMSI using the stored IMSI ↔ $\mathbf{e}_i$ relations.

3. The OEM charges the subscribers.

4. The OEM sends the collected money to the MNO.

In many current billing models, OEMs charge subscribers for vehicular mobile network access. Therefore, our billing model does not require substantial changes to the current state.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	...	23	24
902 (V2X)			MCC			MNC ⟺			PSIN								
3 digits			3 digits			2 – 3 digits			15 – 16 digits								

Figure 3: The structure of a PMSI. The length of the MNC varies as it does in an IMSI. The length of the PSIN varies accordingly, such that the total length sums up to 24 digits.

Subscriber Exclusion.

If a subscriber shows malicious behavior, the subscriber must be excluded from V2X communication. The formal and legal process behind subscriber exclusion is out of scope of this work. However, we assume the MNO knows the PMSI of the violator. To exclude a subscriber, MNOs and OEMs can cooperate, executing the following steps:

1. The MNO sends $\mathbf{e}_i \in \mathcal{E}_{\text{OEM}}$, where PMSI_i matches the violator's PMSI, to the OEM over a connection secured with a session key K_{SESSION}.

$$\text{MNO} \xrightarrow{K_{\text{SESSION}}} \text{OEM} : \mathbf{e}_i$$

2. The OEM determines the set $\mathcal{S}_{\text{IVS}}$ which contains $\mathbf{e}_i$ and maps $\mathcal{S}_{\text{IVS}}$ to the violator's IMSI. The OEM sends the IMSI and $\mathcal{S}_{\text{IVS}}$ back to the MNO.

$$\text{OEM} \xrightarrow{K_{\text{SESSION}}} \text{MNO} : \text{IMSI}$$
$$\text{OEM} \xrightarrow{K_{\text{SESSION}}} \text{MNO} : \mathcal{S}_{\text{IVS}}$$

3. The MNO revokes the received IMSI permanently. The MNO also extracts the PMSIs from $\mathcal{S}_{\text{IVS}}$ and revokes those PMSIs for the current billing period. Consequently, the MNO excludes the violator from the mobile network.

Structure of a PMSI.

A PMSI, as depicted in Figure 3, consists of 24 digits and is similar to an IMSI. The first three digits in an IMSI represent the Mobile Country Code (MCC). However, an IMSI consists of 15 digits only, which does not scale with our increased need for regularly changing pseudonymous identifiers. Therefore, we use the currently unused MCC *902* as an identifier for "V2X" in our PMSI. This way, IMSIs and PMSIs can be distinguished. The next three digits represent the actual MCC of the PMSI. The next two to three digits, the Mobile Network Code (MNC), identify the MNO the PMSI belongs to. Together, the MCC and MNC make up the PLMN. The PLMN identifies a subscriber's home network, which e. g., enables roaming. The remaining 15 - 16 digits of the PMSI represent a unique subscriber identifier, the *Pseudonymous Subscriber Identification Number* (PSIN). As the number of different PSINs is limited, we restrict their validity to billing periods to allow reusability. Since each PMSI is linked to a secret key K_{PMSI}, MNOs can reuse PMSIs by creating a new secret key K_{PMSI} for each PMSI in each billing period. Consequently, IVSs cannot connect to the mobile network with an invalid combination of PMSI and K_{PMSI}. Therefore, this approach scales with a large number of vehicles and relatively rapid changes of

PMSIs: assuming a 15 digit PSIN and a billing period of one month, our scheme can distribute 10^{15} different PMSIs each billing period for each PLMN prefix, thus serving over 20,000,000,000 vehicles for a billing period of one month and a PMSI change every minute for each PLMN prefix.

7.1.2 IMEI

We introduce the *Pseudonymous Mobile Station Equipment Identity* (PMEI), a pseudonym replacing the IMEI. The creation, distribution and use of PMEIs encompasses the following aspects:

Initial Setup.

The OEM supplies each IVS with PMEIs during the manufacturing process:

1. The OEM creates a set of m PMEIs, the OEM's *PMEI pool* $\mathcal{I}_{\text{OEM}}$:

   $$\mathcal{I}_{\text{OEM}} = \bigcup_{i=1}^{m} \{\text{PMEI}_i\},$$

   where $\text{PMEI}_i \neq \text{PMEI}_j$ for all $i \neq j$ and m is a sufficiently large number, depending on the number of subscribers the OEM supplies with PMEIs and the pseudonym change frequency.

2. The OEM registers these PMEIs with the MNO using a secure connection.

   $$\text{OEM} \xrightarrow{K_{\text{SESSION}}} \text{MNO} : \mathcal{I}_{\text{OEM}}$$

3. The OEM distributes a random subset of previously unused elements of its PMEI pool

   $$\mathcal{I}_{\text{IVS}} \subseteq \mathcal{I}_{\text{OEM}}$$

   to each IVS during the manufacturing process in a secure environment. The size of $\mathcal{I}_{\text{IVS}}$ matches the size of $\mathcal{E}_{\text{IVS}}$ distributed to each IVS in Section 7.1.1. The OEM stores the mapping between $\mathcal{I}_{\text{IVS}}$ and the IVS's IMEI and marks the elements in $\mathcal{I}_{\text{IVS}}$ as used.

   $$\text{OEM} \longrightarrow \text{IVS} : \mathcal{I}_{\text{IVS}}$$

PMEI Generation.

Each billing period, the OEM repeats steps 1 and 2 of the *Initial Setup* for PMEIs.

PMEI Request.

IVSs require new PMEIs each billing period or if they run out of valid PMEIs. Regular PMEI requests consist of the following steps:

1. The IVS establishes a connection to the MNO, using a PMEI if necessary. Consequently, the IVS utilizes this connection to establish a secure connection to the OEM as described for the *PMSI Request* in Section 7.1.1. A symmetric cipher scheme using key K_{IVS} protects the confidentiality of all exchanged messages between the IVS and the OEM against third parties and the MNO. The IVS sends its IMEI and requests new PMEIs.

   $$IVS \xrightarrow{K_{\text{IVS}}} \text{OEM} : \text{IMEI}$$

2. The OEM selects a previously unused subset

   $$\mathcal{I}_{\text{IVS}} \subseteq \mathcal{I}_{\text{OEM}}$$

   of its PMEI pool and stores the relation between $\mathcal{I}_{\text{IVS}}$ and the IVS's IMEI. The OEM marks the elements in $\mathcal{I}_{\text{IVS}}$ as used.

3. The OEM sends $\mathcal{I}_{\text{IVS}}$ to the IVS over the aforementioned secure channel using K_{IVS}.

   $$\text{OEM} \xrightarrow{K_{\text{IVS}}} : \mathcal{I}_{\text{IVS}}$$

Regular Operation.

Like with the PMSIs, the IVS changes PMEIs when changing other pseudonyms.

Device Revocation.

If the necessity arises to revoke an IVS's capability to connect to the mobile network, the MNO and the OEM can cooperate. Device revocation becomes necessary when, e. g., a vehicle is stolen or when the ITS detects malicious behavior of an IVS.

1. The MNO sends the PMEI in question to the OEM.

   $$\text{MNO} \xrightarrow{K_{\text{SESSION}}} \text{OEM} : \text{PMEI}$$

2. The OEM identifies the set $\mathcal{I}_{\text{IVS}}$ which contains the received PMEI. The OEM maps $\mathcal{I}_{\text{IVS}}$ to the according IMEI and sends the IMEI and $\mathcal{I}_{\text{IVS}}$ to the MNO. The OEM does not issue new PMEIs to the IVS in question if the IVS should make a request.

   $$\text{OEM} \xrightarrow{K_{\text{SESSION}}} \text{MNO} : \text{IMEI}$$
   $$\text{OEM} \xrightarrow{K_{\text{SESSION}}} \text{MNO} : \mathcal{I}_{\text{IVS}}$$

3. The MNO revokes all corresponding PMEIs for the current period and the corresponding IMEI. A a consequence, the MNO can deny all services to devices using the PMEI in question.

Please note that device revocation, like in regular LTE, fails, if an attacker manages to manipulate his IVS into using arbitrary PMEIs or IMEIs, possibly even causing denial of service for other subscribers.

Structure of a PMEI.

Regular IMEIs consist of 15 digits (see [7] for additional information). Our PMEI is 32 digits long and begins with an eight digit “V2X” identifier, which is identical for all IVSs. The remaining 24 digits are a unique pseudonymous identifier for each billing period. For optimal privacy, these PMEIs should be chosen randomly among all possible 10^{24} combinations and “registered” anonymously by each OEM, such that each PMEI remains unique within each billing period. A simple scheme which distributes fixed sets of PMEIs to each OEM might endanger the privacy of ITS users by serving as an identifier. Setting up an according procedure is out of scope of this work, however.

7.1.3 IP

The IVS shall renegotiate its IP address simultaneously with each change of the IVS's pseudonyms (i. e., the IVS shall stop using its IP address before switching its PMSI and PMEI and fetch a new IP address afterwards).

7.1.4 MSISDN

We can avoid this identifier altogether, since we do not require reachability of IVSs via telephone number (cf. Section 6).

7.1.5 GUTI and C-RNTI

The GUTI and the C-RNTI both serve as temporary identifiers distributed regularly by the mobile network to UEs. Since IVSs and MNOs can negotiate these temporary identifiers using only pseudonyms, GUTIs and C-RNTIs do not require any further action. By contrast, they are supposed to preserve the privacy of subscribers against third party attackers in regular LTE.

7.2 Push Services

The scheme we propose makes it difficult for service providers to address subscribers, since using pseudonymous identifiers makes addressing subscribers impossible without further mechanisms. However, push services can be realized in the following way: After an IVS changes its IP address, it contacts its push service providers and notifies them of the new IP address, using confidential connections. Thus, service providers can use the IVS's current IP address to implement their push services. This also enables IVSs to send messages to other IVSs via a common service.

7.3 LTE Specific Requests

In regular LTE, UEs answer to *Paging Requests* matching the UE's related IMSI. This causes loss of location privacy, since answering a paging request implies that the UE is located within a specific area. Therefore, IVSs shall only answer paging requests related to PMSIs, not to IMSIs.

Furthermore, MNOs can issue *Identity Requests* to their UEs. UEs answer this request with their IMSIs or IMEIs. Since this clearly violates privacy requirements, IVSs following our scheme shall answer with pseudonyms instead.

7.4 MBMS

A likely candidate for cell broadcasts is Multimedia Broadcast Multicast Service (MBMS). To the best of our knowledge, no version of cell broadcast is currently supported in commercial LTE networks. For the MBMS to work, all participants need an MBMS user key [1]. To avoid identification of participants, all subscribers of a MNO shall share the same MBMS user key. V2X related cell broadcasts are non-confidential, thus this does not pose a risk for confidentiality.

8. ANALYSIS OF THE SCHEME

In our analysis, we evaluate whether our proposed scheme fulfills the requirements given in Section 6. In our threat analysis in Section 4, we identified two possible attackers whose capabilities exceed those of any third party: MNOs and OEMs. Therefore, we focus on these more capable attackers in the following analysis.

In our scheme, MNOs create PMSIs. However, OEMs distribute encrypted PMSIs to IVSs without revealing the identity of the receiving IVSs to MNOs. Therefore, MNOs cannot map PMSIs to IMSIs. Likewise, OEMs cannot decrypt the distributed PMSIs, preventing them from mapping PMSIs to IMSIs as well. While OEMs can map PMEIs to IMEIs, PMEIs are usually not transmitted in plain text between IVSs and MNOs, such that OEMs cannot use PMEIs to track IVSs. MNOs, on the other hand, cannot map PMEIs to IMEIs, since IMEIs are again distributed by OEMs. Since IVSs change PMSIs, PMEIs and IP addresses simultaneously, no linking between pseudonyms is feasible without additional information, like, e. g., data transmitted between IVSs and service providers or observing vehicles directly.

R1 **Location privacy.** Our scheme protects the location privacy of subscribers against MNOs, since MNOs cannot match PMSIs to subscriber identities. This holds true as long as the PMSI change frequency is high enough and the PMSI pool of an OEM is large enough to grant sufficient pseudonymity for IVSs and thus for subscribers. Note that the PLMN inside the PMSI can become an identifier, e. g., when an IVS is located in a foreign country. Therefore, foreign MNOs in case of roaming, are likely able to track IVSs while they are moving within these MNOs's networks. However, the use of GUTIs still protects the location privacy of subscribers against OEMs or third party attackers. Furthermore, our scheme also protects location privacy against OEMs in general, since OEMs do not gain any knowledge of the PMSIs they actually distribute to IVSs. This holds true because the PMSIs are encrypted with a newly generated key in each billing period by each MNO. In order to get this key, OEMs would have to read this key from a valid UICC distributed by the according MNO. However, we assume that the hardware of the UICC and the USIM are certified and protected against hard- and software attacks respectively. Thus, we consider these keys secure from attacks by OEMs. Since the PMSIs are not known to OEMs, they cannot track IVSs, even if they managed to listen to all communication exchanged between IVSs and their MNOs.

R2 **Usage privacy.** Our scheme enhances usage privacy, since OEMs aggregate billing information without having knowledge of the used services, while MNOs cannot match PMSIs to subscriber identities. The choice to have OEMs collect the money further enhances the effect of aggregation. However, we note that the billing information received by OEMs might leak some knowledge, e. g., when characteristic costs imply roaming, the OEM gains knowledge about a stay abroad. However, since MNOs aggregate billing information for each PMSI before sending it to OEMs, this effect should be minor in most cases. Note that this scheme prevents detailed bills for subscribers, so there is a tradeoff between subscriber privacy and information. Several possible solutions for solving this issue may exist; however, this is out of scope for this work.

R3 **Pull services.** As shown in Section 7, our scheme allows IVSs to establish connections just as with regular LTE. Therefore, pull services, which require the service user to actively initiate connections, work without additional mechanisms. Note that regularly contacting a set of services constitutes an identifier, which might enable MNOs to link pseudonymous identities and thus break privacy requirements. However, since using services happens at the discretion of subscribers, this issue is out of scope for this work.

R4 **Push services.** The active notification of service providers after each change of pseudonymous identifiers, as described in Section 7, allows the use of push services. This does not enable service providers to track their subscribers, since only the IP addresses of their subscribers become known to them. Since the communication on the wireless medium is encrypted between MNOs and IVSs, listening on the wireless medium does not suffice to track subscribers based on IP addresses. The only identifier transmitted in plain text is the PMSI, which is unknown to service providers. Again, all remarks concerning identifiers as in *pull services* apply.

R5 **Reachability of IVSs via cell broadcast.** IVSs using our scheme are members of cells just like in regular LTE. Therefore, our scheme does not affect cell broadcasts at all.

R6 **Support of billing.** Our scheme supports billing by combining the knowledge of OEMs and MNOs as shown in Section 7. We expect laws and interest in brand integrity to keep both OEMs and MNOs from committing billing fraud.

R7 **No compromise of security by the scheme.** Our scheme focuses on identifiers in LTE and transmits keys confidentially. All other security aspects are left untouched. As shown above, our scheme enhances subscriber *privacy* compared to regular LTE.

We do not affect the inherent security mechanisms in terms of *integrity* and *authenticity*. This holds true because attackers cannot obtain PMSIs without a valid IMSI and related shared key K_{IMSI}. Furthermore, attackers cannot forge valid identities, since PMSIs are linked to secret keys K_{PMSI} obtained in the PMSI request process as described in Section 7.1.1. Finally, the mutually shared key K_{IVS} between OEMs and IVSs secures the transmission of the IVS's PMSI pool $\mathcal{E}_{\mathrm{IVS}}$ from OEMs to IVSs, preventing attackers from sniffing $\mathcal{E}_{\mathrm{IVS}}$ on the wireless link.

Our scheme does not affect the protection of *confidentiality* against third parties. However, OEMs might try to use their role in our scheme to attack the confidentiality of IVSs's communication over the mobile network. On the one hand, OEMs might subscribe to one or more MNO's services. OEMs could then distribute arbitrary elements from their PMSI pools to these USIMs, especially PMSIs that were already distributed to "real" subscribers. Given K_{PERIOD}, which any subscriber receives from their MNO, this UICC could try to decode replayed messages sent on the wireless link between an IVS and an MNO. However, since LTE features replay protection, OEMs would also have to manipulate the USIMs on these UICCs, since otherwise the USIMs would realize the replay attempt and contact the real infrastructure for fresh information. Using a UICC that was created by an OEM does not work either, since it is lacking the shared secret key related to the IMSI which is handed out by MNOs to their subscribers. On the other hand, OEMs might attempt to extract K_{PERIOD} from a regular UICC to decrypt their PMSI pool, thus extracting all keys and PMSIs. However, we require UICCs to be protected against hardware attacks. Therefore, extracting keys from UICCs requires a vast investment in terms of time and money. Even if OEMs managed to successfully execute this attack, they would have to eavesdrop on the GUTI negotiation step, where PMSIs and their related keys are actually used and a new key is established between IVS and MNO. In turn, OEMs would require a huge listening infrastructure to reliably eavesdrop on this step. Thus, given the risk of discovery and the probable consequences in terms of law suits and image loss for the brand, we consider this kind of attack highly unlikely.

Replacing the shared key K_{PERIOD} in an alternate scheme, where the MNO encrypts each PMSI pair for individual IVSs, creates other issues: Either, the MNO shares the key for an individually encrypted PMSI pair with an individual IVS, which violates the IVS's privacy, enabling the MNO to link the PMSI pair to the IVS. Or, the MNO creates an individually encrypted version of each PMSI pair for each IVS, and the OEM sends all these encrypted versions of a single PMSI pair to the IVS, which in turn decrypts the single version encrypted with the IVS's key. Clearly, this approach does not scale well with the expected amount of subscribers. Furthermore, the MNO could cheat by encrypting specific sets of PMSI pairs for each IVS, breaking privacy.

R8 **Minimize changes to the LTE standard.** Our scheme introduces the PMSI, which requires the mobile network to handle mobile subscriber identities containing the specific MCC *902*, signaling "V2X", differently than regular IMSIs or GUTIs. However, the handling of a PMSI is fairly straight forward as it basically demands parsing the actual PLMN information, which follows the regular pattern, and a longer than usual identifier following the PLMN information. Analogously, the PMEI is longer than a regular IMEI. Nevertheless, handling the PMEI does not require changes to the protocol, but only parsing a longer number for the specific "V2X" prefix. Other than that, our proposed scheme does not require any substantial changes to LTE, but mainly additional communication between MNOs and OEMs over regular internet connections. Therefore, our scheme only requires minimal changes to LTE. These changes are necessary, since an overlay approach cannot mask permanent identifiers, such as the IMSI, from the MNO.

9. CONCLUSION

We showed that LTE in vehicular communication, while offering great advantages, has potential implications for the privacy of ITS users. Our proposed scheme solves these issues with minimal changes to LTE standards. We distributed identity management between MNOs and OEMs, replaced identifiers with pseudonyms and developed protocols for the management of these pseudonyms. Thus, our scheme enables the use of LTE in V2X communication without undermining the carefully crafted privacy-preserving design of G5 communication.

10. ACKNOWLEDGMENTS

This work was funded within the project CONVERGE by the German Federal Ministries of Education and Research as well as Economics and Technology.

11. REFERENCES

[1] 3GPP. TS 31.102: Characteristics of the Universal Subscriber Identity Module (USIM) application. http://www.3gpp.org/ftp/Specs/html-info/31102.htm, 2012.

[2] E. E. . 663. Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz band, 2009.

[3] M. Arapinis, L. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon, and R. Borgaonkar. New Privacy Issues in Mobile Telephony: Fix and Verification. 2012.

[4] H. Choudhury, B. Roychoudhury, and D. K. Saikia. Enhancing User Identity Privacy in LTE. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, pages 949–957. IEEE, 2012.

[5] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard), Aug. 2008. Updated by RFCs 5746, 5878, 6176.

[6] ETSI. Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (3GPP TS 24.008 version 8.6.0 Release 8), July 2009. `http://www.etsi.org/deliver/etsi_ts/124000_124099/124008/08.06.00_60/ts_124008v080600p.pdf`.

[7] ETSI. Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003 version 11.4.0 Release 11), December 2012. `http://www.etsi.org/deliver/etsi_ts/123000_123099/123003/11.04.00_60/ts_123003v110400p.pdf`.

[8] ETSI. Universal Mobile Telecommunications System (UMTS); Radio interface protocol architecture (3GPP TS 25.301 version 11.0.0 Release 11), September 2012. `http://www.etsi.org/deliver/etsi_ts/125300_125399/125301/11.00.00_60/ts_125301v110000p.pdf`.

[9] ETSI. Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Security architecture (3GPP TS 33.102 version 11.5.0 Release 11), February 2013. `http://www.etsi.org/deliver/etsi_ts/133100_133199/133102/11.05.00_60/ts_133102v110500p.pdf`.

[10] L. Le, A. Festag, R. Baldessari, and W. Zhang. Vehicular wireless short-range communication for improving intersection safety. *Communications Magazine, IEEE*, 47(11):104 –110, November 2009.

[11] National Institute for Science and Technology (NIST). Advanced Encryption Standard (FIPS PUB 197), November 2001. `http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf`.

[12] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux. Secure vehicular communication systems: design and architecture. *Communications Magazine, IEEE*, 46(11):100 –109, November 2008.

[13] C. Sankaran. Network access security in next-generation 3GPP systems: A tutorial. *Communications Magazine, IEEE*, 47(2):84–91, 2009.

[14] J. Wedel, B. Schunemann, and I. Radusch. V2X-Based Traffic Congestion Recognition and Avoidance. In *Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on*, pages 637 –641, dec. 2009.

GLOSSARY

The following listing contains the most important abbreviations used throughout this document:

OEM	Original Equipment Manufacturer
MNO	Mobile Network Operator
ITS	Intelligent Transportation System
IVS	ITS Vehicle Station
IMSI	International Mobile Subscriber Identity
IMEI	International Mobile Station Equipment Identity
GUTI	Globally Unique Temporary ID
PMSI	Pseudonymous Mobile Subscriber Identity
PMEI	Pseudonymous Mobile Station Equipment Identity
UE	User Equipment
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module
PLMN	Public Land Mobile Network
MCC	Mobile Country Code
MNC	Mobile Network Code