A Survey of Security and Privacy Issues in V2X Communication Systems

TAKAHITO YOSHIZAWA, imec-COSIC KU Leuven, Belgium
DAVE SINGELÉE, imec-COSIC KU Leuven, Belgium
JAN TOBIAS MÜHLBERG, imec-DistriNet, KU Leuven, Belgium
STÉPHANE DELBRUEL, LaBRI, University of Bordeaux, France
AMIR TAHERKORDI, Informatics Department, University of Oslo, Norway
DANNY HUGHES, imec-DistriNet, KU Leuven, Belgium
BART PRENEEL, imec-COSIC KU Leuven, Belgium

Vehicle-to-Everything (V2X) communication is receiving growing attention from industry and academia as multiple pilot projects explore its capabilities and feasibility. With about 50% of global road vehicle exports coming from the European Union (EU), and within the context of EU legislation around security and data protection, V2X initiatives must consider security and privacy aspects across the system stack, in addition to road safety. Contrary to this principle, our survey of relevant standards, research outputs, and EU pilot projects indicates otherwise; we identify multiple security and privacy related shortcomings and inconsistencies across the standards. We conduct a root cause analysis of the reasons and difficulties associated with these gaps, and categorize the identified security and privacy issues relative to these root causes. As a result, our comprehensive analysis sheds lights on a number of areas that require improvements in the standards, which are not explicitly identified in related work. Our analysis fills gaps left by other related surveys, which are focused on specific technical areas but not necessarily point out underlying root issues in standard specifications. We bring forward recommendations to address these gaps for the overall improvement of security and safety in vehicular communication.

CCS Concepts: • **Security and privacy** → *Distributed systems security*; **Mobile and wireless security**; **Distributed systems security**; **Mobile and wireless security**; **Pseudonymity, anonymity and untraceability**; **Privacy-preserving protocols**; **Domain-specific security and privacy architectures**; **Privacy protections**; *Social aspects of security and privacy*; *Usability in security and privacy*; • **Networks** → **Network privacy and anonymity**; **Wireless access networks**; **Mobile and wireless security**.

Additional Key Words and Phrases: Security, Privacy, V2X, Vehicular communication, ITS standard, EU projects

Authors' addresses: Takahito Yoshizawa, imec-COSIC KU Leuven, Kasteelpark Arenberg 10 Bus 2452, Leuven, B-3001, Belgium, takahito.yoshizawa@esat.kuleuven.be; Dave Singelée, imec-COSIC KU Leuven, Kasteelpark Arenberg 10 Bus 2452, Leuven, B-3001, Belgium, dave.singelee@esat.kuleuven.be; Jan Tobias Mühlberg, imec-DistriNet, KU Leuven, Celestijnenlaan 200a box 2402, Leuven, B-3001, Belgium, jantobias.muehlberg@cs.kuleuven.be; Stéphane Delbruel, LaBRI, University of Bordeaux, Cours de la Libération, 351, Talence, F-33405, France, stephane.delbruel@labri.fr; Amir Taherkordi, Informatics Department, University of Oslo, Gaustadalléen 23B, Oslo, 0373, Norway, amirhost@ifi.uio.no; Danny Hughes, imec-DistriNet, KU Leuven, Celestijnenlaan 200a box 2402, Leuven, B-3001, Belgium, danny.hughes@cs.kuleuven.be; Bart Preneel, imec-COSIC KU Leuven, Kasteelpark Arenberg 10 Bus 2452, Leuven, Belgium, bart.preneel@esat.kuleuven.be.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2022 Association for Computing Machinery.
0360-0300/2022/8-ART $15.00
https://doi.org/10.1145/3558052

Just Accepted

1 INTRODUCTION

1.1 Overview

Vehicular communication has gained momentum in the past years. It is expected that progress of this communication technology will have a major impact on the automotive industry and in particular on how vehicles are driven in society. Vehicle-to-Everything (V2X) communication is expected to bring numerous benefits. According to the assessment by National Highway Traffic Safety Administration (NHTSA) in the US [86], the adoption of Vehicle-to-Vehicle (V2V) technology is expected to improve the overall traffic safety by preventing 439,000 to 615,000 accidents, saving 987 to 1366 lives, and eliminating 537,000 to 746,000 property damage incidents per year. A report by the European Commission (EC) [10] states that the overall benefits of deploying Cooperative Intelligent Transport System (C-ITS) include reduced travel times, increased efficiency, reduced accident rates, and savings in fuel consumption.

The first standardized V2X technology is based on IEEE 802.11p (IEEE 802.11 Outside the Context of Basic Service Set (OCB) mode). In the US, the V2X system using 802.11 OCB mode is called Dedicated Short-Range Communication (DSRC) and its upper layer is called Wireless Access in Vehicular Environment (WAVE) as specified in the IEEE 1609 series and the SAE International (SAE) standard J2735 [98] (formerly the Society of Automotive Engineers). In Europe, ITS systems based on IEEE 802.11 OCB mode are called Intelligent Transport System G5 (ITS-G5), and its upper layer is referred to as C-ITS. Detailed descriptions of these standards and how they relate to each other are discussed in [114]. An overview of the V2X communication system is shown in Figure 1. V2X is a collective term which includes multiple communication modes:

- Vehicle-to-Vehicle (V2V): direct communication between vehicles.
- Vehicle-to-Infrastructure (V2I): communication between a vehicle and the infrastructure such as traffic light.
- Vehicle-to-Person/Pedestrian (V2P): between a vehicle and other road users such as pedestrians or cyclists.
- Vehicle-to-Network (V2N): between a vehicle and network entities via a mobile network base station.
- Infrastructure-to-Network (I2N): between an infrastructure and network entities via a mobile network.

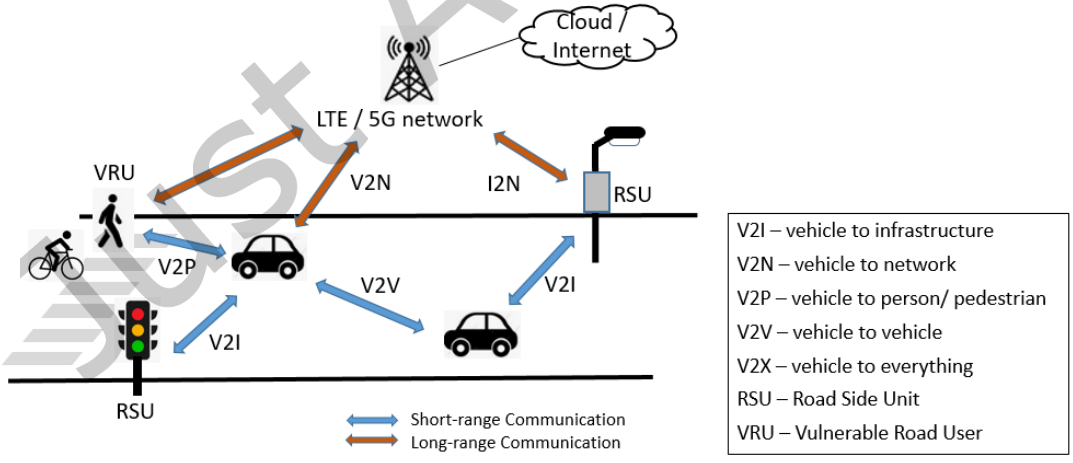

Fig. 1. Overview of V2X Communication System

Meanwhile, modern vehicles are equipped with increasing number of Electronic Control Units (ECUs), embedded computers with the power to sense and actuate within the vehicle. Today, standard automobiles have

Just Accepted

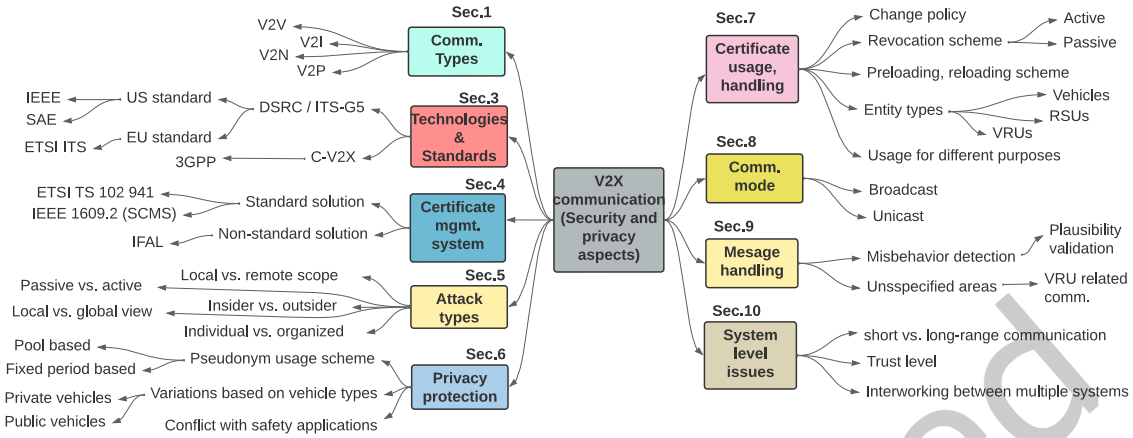

Fig. 2. Overview of Security and Privacy Aspects in V2X Systems.

more than 80 ECUs; luxury ones have as many as 150 ECUs [80, 107]. Their software size amounts to 100 million lines of code (LoC), far exceeding that of the space shuttle (400,000 LoC), F35 fighter jet (23 millin LoC) and even the Hadron Collider (50 million LoC) [108]. The increased complexity of vehicular ICT—ECUs, connectivity, overall software size—implies an overall increasing digital attack surface and thereby increasing security and privacy risks. Contrary to this point, the Controller Area Network (CAN) bus in vehicles does not support protection against cyberattacks; it does not support authentication and message integrity functionalities [83]. In fact, the CAN design is based on the assumption that it operates in a friendly environment where no security threats exist [13]. Yet, real-life attack scenarios around CAN communication and software defects in ECUs and their consequence as potential road hazard raise immediate concerns [22, 70, 81, 83]. Even if a relatively small number of vehicles on the road are directly affected by an attack, the consequences for road safety and national infrastructures can be devastating [112]. Therefore, vehicular communication technologies need to be secure, robust, and resilient to be truly beneficial. In this sense, including security and safety requirements from the initial stage of the system design is essential [83]. Ensuring secure communication requires at least mechanisms for authentication and integrity protection, which allows communicating parties to verify each other's identity, and the authenticity of messages: a vehicle is indeed a vehicle and a traffic light is indeed a traffic light, and communication between these entities cannot be spoofed or otherwise manipulated. In addition, protecting the *privacy* of vehicle owners is equally important. If no privacy protections are implemented on top of authenticated communications, vehicles can be tracked remotely, and information about drivers and their personal behaviour can be inferred by authorities, infrastructure operators and adversaries. In the V2X context, privacy-preserving technologies rely on the use of pseudonymous identities. These schemes come with their own security and safety challenges [73, 97], and a number of proposals to mitigate these challenges have been published [17, 74, 82], but not necessarily adopted by standardizing bodies.

This article surveys recent efforts in research and standardization regarding security and privacy aspects of V2X communication. We aim to provide a comprehensive overview of these aspects from the perspective of the ETSI ITS specifications, and link this to the objectives and results of recent research, development, and integration actions, specifically in the European Union but with links to other markets and political bodies. As a key contribution, our survey highlights a range of shortcomings and imprecisions in ongoing standardization efforts, and points towards potential solutions and open research questions regarding these security and privacy issues. As such, our article targets policy makers, researchers, and standardization engineers. Specifically for

Just Accepted

these actors, we provide the background to assess the novelty and relevance of research, and a medium to identify domains of research with a potentially high impact on upcoming standardization or regulatory efforts. Figure 2 gives an overview of these domains and links them to the structure of this article.

1.2 Methodology and Contributions

In this article, and in reference to related work summarized in Sec. 2, we focus on security and privacy aspects of European Union (EU) initiatives across a range of European pilot activities, such as past or present V2X-related EU projects, and analyse ETSI ITS specifications from security and privacy perspectives. Our focus on EU standard and projects is due to several reasons: (1) Europe is the largest exporter of vehicles equipped with communication technologies as many major vehicle manufacturers are based in Europe, (2) covering relevant projects in other regions such as the US will diminish the focused analyses, and (3) including analysis of other regions will likely result in excessively long paper while adding relatively marginal additional benefit.

As a result, we identify a number of gaps in the ETSI ITS standards which stem from incoherent and inconsistent specifications. Based on our root cause analysis of the reasons and difficulties associated with these gaps, we provide recommendations based on our findings. We also identify previously unreported security and privacy issues resulting from recent trends driven by C-V2X such as the convergence of vehicular communication and mobile systems; one notable example being the absence of security and privacy considerations in the integration of smartphone in the ITS system in V2P scenarios. For many of these issues, existing literature offers either no solution or inadequate ones. When applicable, we propose ideas for potential solutions as an agenda for future analysis and investigation. We believe our findings are fundamental and essential to ensure that V2X communication is secure and protect user privacy.

We focus primarily on the EU initiatives in this paper. However, subtle but important contrast emerges as we put differences of the solutions between the EU and the US in perspective because the security and privacy solutions in two systems are similar in high level but different in details. For this reason, we discuss the similarities and differences between the two standards as the foundation of our discussion. When terminologies are different between the systems, we use the EU terminology unless it is necessary to explicitly describe the US system.

1.3 Document Organization

This paper is organized as follows. We first set a baseline of the discussion by summarizing the related survey papers and EU projects in Sec. 2, describing the overview of V2X technologies and their standards in Sec. 3. Then, we discuss their security management systems in Sec. 4. In Sec. 5, we discuss threat model that we use as a base of our analysis. Starting from Sec. 6 and up to Sec. 10, we examine details of specific security aspects and gaps. In Sec. 11, we present our root cause analysis of key gaps that need further study and research, and put forward recommendations. We conclude our study in Sec. 12. As a guide for the rest of this paper, Figure 2 provides an illustration of the various security and privacy protection-related aspects covered in this paper.

2 RELATED WORK

We first review related work of V2X communication.[1] In the past years, a number of survey papers on security and privacy aspects of V2X have been published. The purpose of this section is to highlight the differences of our work compared to them. These survey papers can be categorized into three groups: ① discussion and solutions for generic vehicular network, ② surveys that cover both DSRC and C-V2X based solutions, and ③ surveys that focus specifically on C-V2X solutions.

In the first group, Hasan et al. [60], van der Heijden et al. [109], and Bißmeyer [14] exclusively focus on misbehaviour detection. In [60], a large part of this survey is dedicated to the discussion on attack and misbehaviour

[1] An extended version of this section is available in the online supplemental material, including both relevant survey papers and EU projects.

Just Accepted

detection mechanisms by classifying and comparing numerous proposals on this subject. Survey in [109] provides in-depth analysis of detection mechanisms, and classify them into two-dimensions. The first dimension is *node-centric vs. data-centric*; the second dimension is *autonomous vs. collaborative*. Based on this classification, misbehaviour detection mechanisms can be categorized into one of the four types. The work in [14] focuses in two main areas: 1) misbehaviour detection, and 2) attacker identification in both local short-term and central long-term scope.

The survey by Badea and Stanciu [11] has a limited focus on security and privacy aspects. The only security related topic is on specific use cases and scenarios such as car sharing. Similarly, Ometov and Bezzateev [89] is not a survey; it is a proposal to apply multi-factor authentication (MFA) in V2X communication. This solution uses reversed Lagrange polynomial from Shamir's secret sharing schema as the building block. Wang et al. [113] focus specifically on the certificate revocation schemes in V2X communication. They analyse and classify them based on location where the revocation information has been placed. The entire revocation process is then divided into three stages: 1) resolution, 2) distribution, and 3) the use of revocation information.

In the second group, Huang et al. [61] treat both security and privacy topics although it is a small part of their paper as the content provides overview of 3GPP specifications on both LTE and 5G-based C-V2X rather than a survey. For security aspect, they discuss basic security services and attack types in vehicular networks, then categorize security solutions from two perspectives: 1) cryptography-based schemes, and 2) trust-based schemes. For privacy solutions, they categorize them into two types: 1) identity privacy preservation, and 2) location privacy preservation. Alnasser et al. [8] analyse security threats and solutions for both DSRC and LTE-based C-V2X. Their threat analysis includes availability, integrity, confidentiality, authenticity, and non-repudiation aspects. Then, they categorize security solutions including cryptography-based, behaviour/trust-based, and identity-based solutions. Ghosal and Conti [58] provide overview and background of both DSRC/WAVE and 3GPP-based LTE and 5G C-V2X systems, then discuss security challenges by analysing various attack types and how they impact V2X communication. Later, they examine techniques and solutions in specific areas, including symmetric key cryptography, privacy preservation, message authentication.

In the third group, Cao et al. [18] cover overall 5G system security and related topics rather than focusing on 5G-based C-V2X. They describe security and privacy aspects of other vertical applications such as IoT, device-to-device (D2D), and 5G-specific topics such as network slice. Only one section (Sec.VI) is dedicated to security in both LTE and 5G-based C-V2X solutions. In it, security requirements, solutions, and open issues are discussed. Muhammad and Safdar [82] focus specifically on the authentication mechanism in the context of LTE C-V2X. They enumerate attack types and describe their relevance and corresponding countermeasures. They discuss multiple proposed authentication solutions and analyse how they can meet the needs of C-V2X communication. Lu et al. [74] focus on security and privacy aspects of LTE and 5G-based C-V2X. Their survey is on challenges in trust, security, and privacy-related issues in C-V2X, followed by discussions on strategies to resolve them. The discussion in Lai et al. [72] rather narrowly focuses on a specific C-V2X scenario (platooning) rather than more general V2X communication. They propose security solutions, including privacy-preserving platoon group set up, distributed group key management, and cooperative message authentication. Marojevic [78] focuses on LTE-based C-V2X, discusses its threat scenarios, lists out associated security requirements, and proposes research directions to satisfy these requirements, along with the needs of further standardization to ensure security mechanisms are in place. In summary, the examined surveys can be characterized as follows:

- Analysis of relevant threat scenarios and attack types and their impacts to V2X communication,
- Discussion of issues, challenges, and requirements on specific security areas,
- Discussion on approaches and strategies to address stated issues and requirements,
- Description and comparison of existing proposed solutions on specific security areas,
- A new proposal on specific security or privacy area.

Just Accepted

In contrast to these surveys, as articulated in Sec. 1.2, our unique contribution in this paper is to point out fundamental issues and gaps in the ETSI ITS standards and unreported security and privacy issues that have not been discussed in the existing survey papers.

3 V2X TECHNOLOGIES

In this section, we discuss the two competing V2X standards, the first one being specified by the IEEE and the second by the 3GPP. We introduce these two main competing standards and highlight their differences as we set the context of the standardization in order to explore their respective security aspects and how they differ further in our survey. The discussion on their shared features being out of scope of this survey, we recommend for readers desirous to explore this path a previous study by Yoshizawa et al. [114] focusing on the similarities of these two standards and possible hints on their cohabitation.

3.1 IEEE standard

In 2010, IEEE approved the amendment IEEE 802.11p designed to standardize vehicular communication system. The following publication of the IEEE 802.11 standard in 2016 [62] incorporated the amendment IEEE 802.11p. This amendment also specifies a new operation mode dubbed *Outside Context of a Basic Service Set* (OCB) mode for each 802.11p compliant device to be set to. OCB mode does not need authentication nor association and the only parameter to set is the central channel frequency and the channel bandwidth to communicate. Overall, this amendment concerns the PHY and MAC layers for WLAN-based V2X communications. To build it up towards the applicative layer, the IEEE 1609 standard known as *wireless access in vehicular environments* (WAVE) was developed by IEEE, while in Europe the ETSI committee on *Intelligent Transportation Systems* (ETSI ITS) worked on top of IEEE 802.11p towards standardising applications and a security framework. There are two initiatives benefiting from this work: SAE [98] is known as *Dedicated Short-Range Communications* (DSRC), and ETSI ITS-G5. Both of them define the upper layer protocols that operate on top of the 802.11 OCB mode. The intended application is short-range communication sufficient for direct communication involving both V2V between vehicles and V2I between vehicles and *Road Side Units* (RSUs).

3.2 3GPP standard

Since 2014, the 3rd Generation Partnership Project (3GPP) has worked on standardizing vehicular communication based on previously standardised 4G LTE, and later on included 5G mobile cellular connectivity. This standardisation effort begun with the Proximity Services (ProSe) functionality published in Release-12 which was originally designed for public safety communication. Later in Release-13, support of direct communication between vehicles (D2D) was added. To expand ProSe capabilities towards D2D communications in a cellular environment, a new interface called PC5 was defined in 3GPP TS 23.285 [2] for the LTE system. The equivalent functionality for the 5G system is in 3GPP TS 23.287 [4]. The PC5 interface, also denoted *sidelink*, facilitates a new communication path in addition to the existing *Uu* interface between the User Equipment (UE) and the base station (the terminologies in standard specifications for base station in LTE and 5G are *eNodeB* and *gNodeB*, respectively). This combination of short-range sidelink (PC5) and long-range *(Uu)* communications under the same system is considered complementary and enables a wide range of new types of use cases or services. This technological approach relying on 4G LTE or 5G V2X communications is combined under the 3GPP standard for Cellular V2X (C-V2X).

3.3 Differences between ITS-G5/DSRC and C-V2X

In this section, we highlight conceptual differences between the two competing key V2X standards. For the sake of clarity, the one carried by IEEE comprising IEEE 802.11 OCB mode along with DSRC/ETSI ITS-G5 will be

Just Accepted

designated using its ETSI denomination, i.e. ITS-G5, while the second defined by 3GPP will be specified under the term C-V2X.

3.3.1 Two different target scenarios. The vehicular communication originally envisioned by the IEEE for the ITS-G5 was V2V where vehicles directly communicate with one another. Later on, communication that involves infrastructure, such as RSUs, was added. This type of communication is called V2I and in that scenario both V2V and V2I are designed from the point of view of the vehicle and its communications capabilities.

When the C-V2X concept emerged, it envisioned a scenario introducing two distinct new communication paradigms. One is the involvement of the cellular mobile network (V2N); the other is the involvement of pedestrians or cyclists through the use of smartphones (V2P). The addition of V2N and V2P paradigms is a natural extension to vehicle communication in the context of cellular mobile networks as both short-range and long-range communications in the C-V2X are defined by the same standard body (3GPP).

Collectively, both ITS-G5-based systems and C-V2X-based systems use the term *V2X*. However, the target scenarios are different. In the first one, the focus is on short-range communications involving vehicles and RSUs. Within the context of ITS-G5-based systems, the *Intelligent Transport System - Stations* (ITS-S) consists of only two types: *On-Board Unit* (OBU) and RSU. Thus, only dedicated devices for ITS are envisioned to be part of the vehicular communication system. In this sense, the term *V2X* refers to V2V and V2I from the perspective of ETSI ITS-G5-based systems.

In the C-V2X-based system, inclusion of the mobile network (V2N) and pedestrians and cyclists (V2P) using a smartphone as a new type of ITS-S introduces new dimensions in the vehicular communication. Especially, introducing consumer devices within the family of ITS-S device types extend the range of communication options and use case scenarios. In this sense, the term *V2X* refers to V2V, V2I, V2N, and V2P from the perspective of C-V2X-based systems.

3.3.2 Specific Issues with ITS-G5. Several concerns have been reported regarding the use of ITS-G5/DSRC within the context of vehicular communication. For example, Klingler et al. [69] show that the use of unicast in IEEE 802.11p OCB mode leads to a *Head-of-Line blocking* as each unicast frame requires an acknowledgment from the receiving ITS-S. Absence of acknowledgment in unicast causes subsequent frames to be blocked from transmission, not only to a specific unicast communication but also to other outbound traffic from the ITS-S in question. To create this *Head-of-Line blocking* condition, only a minimally sophisticated attack is necessary as all it requires is to prevent the reception of an acknowledgment frame. Moreover, this condition can occur under the expected normal operating environment in vehicle communication where moving vehicles enters and exists other vehicles' communication range. This point implies that IEEE 802.11 OCB mode-based systems such as ETSI ITS-G5 and DSRC are suitable only for strictly broadcast-based communication in the V2X environment.

Another issue of with 802.11 OCB mode is the lack of reliability and performance in V2X environment. A formal analysis by Ma et al. [75] shows that 802.11 OCB based system is not able to guarantee high reliability due to potential frame collisions and severe channel fading condition. The exponential back-off mechanism used in 802.11 to address frame collision and degraded radio condition has negative performance implications with increasing traffic load. This problem is pronounced further in dynamically moving vehicle environment. In addition, hidden terminal problem is more severe in broadcast than that in unicast. In other words, both broadcast and unicast modes have issues in 802.11-based systems in V2X environment. This is in contrast to the conventional WLAN environment where wireless devices are likely more static compared to vehicles moving at high speed. On the contrary, in mobile systems (e.g. 4G LTE) radio resource is managed by the network. While various cellular protocols use time slotting or time sync to prevent the above-mentioned performance issue, latency comes however at a price.

Just Accepted

3.4 ISO standard

International Standard Organization (ISO) specifies several vehicle-related standards. ISO 26262 [64] defines functional safety of electrical and electronic devices for the automotive industry. It adapts the International Electrotechnical Commission (IEC) 61508 standard, a functional safety standard that defines safety life cycle of electronic systems and products for all industries. It is a risk-based safety standard; vehicles assess the risk of possible hazardous situations and mitigate their impacts to avoid systematic failure of vehicles. It was first published in 2011 and was revised in 2018 [64] in which cybersecurity aspects are added in a limited scope by covering only the interface from functional safety to cybersecurity [102].

ISO/SAE 21434 [65] specifies cybersecurity standard for road vehicles. It started in 2016 as a joint work of ISO and SAE. It is based on SAE J2735 [98]; ISO/SAE 21434 defines a process and minimum criteria for cybersecurity engineering through all phases of product life cycle to prevent cyberattack on vehicles [76]. By complying to this standard, the whole automotive industry follows the uniform cybersecurity development process through the vehicle development life cycle. An analysis by Macher et al. [76] indicates that ISO/SAE 21434 leaves a gap as it stays at an abstract level and is not intended to provide answer to specific implementation details, methods, guidelines, or best practice, and does not present a "silver-bullet" per se. In addition, cybersecurity for autonomous vehicles and non-vehicles such as RSU are outside the scope of this standard.

ISO 39001 [66] is a management system standard for Road Traffic Safety (RTS). It was first published in 2012. Its goal is to improve organizations' traffic safety, and it is targetted for organizations that have a process to improve traffic safety. Organizations that adhere to ISO 39001 can obtain certification of compliance.

4 SECURITY MANAGEMENT SYSTEM OVERVIEW

In this section, we first revisit the security related standards in both the EU and the US. Then we review the security management system defined in these specifications. Both the EU and the US systems are based on a Public Key Infrastructure (PKI) [7]. These ITS security management systems particularly focus on how to manage the certificates for the ITS-Stations (ITS-S). This section highlights the similarities and differences between security management systems in the EU and the US as a baseline for the discussion in the following sections.

4.1 ETSI C-ITS and IEEE 1609.2

The most notable security-related ITS specifications are listed in Table 1. The certificate management system adopted in the US is specified in IEEE 1609.2 [63]. It is called Security Credential Management System (SCMS). A comprehensive and detailed description of the SCMS is found in Brecht et al. [17]. The ETSI ITS standard covers a range of aspects across separate documents. Among them, ETSI TS 102 940 [46] defines the overall architecture of C-ITS security management system. Figure 3 illustrates the overall security management system and the relationship among the entities within the system, including the definition of reference points (e.g. S1, S2), following [46]. Key entities include:

- Root CA (RCA) — This entity is the root of trust of the entire ITS certificate management system. One or more RCA issues certificates to the EA and AA.
- Enrollment Authority (EA) — This entity accepts enrollment requests from the ITS-S and issues enrollment credentials that are used by the ITS-S to contact the AA.
- Authentication Authority (AA) — This entity verifies the successful enrollment based on the enrollment credential issued by the EA, and issues one or more Authorization Certificates, which is also referred to as an Authorization Ticket (AT). The AT is equivalent to a pseudonym certificate in general term.
- ITS Station (ITS-S) — This entity is the end device and the user of ATs issued by the AA. It includes multiple types of devices such as an On-Board Unit (OBU) in the vehicle, a Road Side Unit (RSU), and other types of devices that are engaged in the V2X communication.

Just Accepted

Table 1. US AND EU ITS SPECIFICATIONS (SECURITY SPECIFIC)

Spec #	Title	Latest Version	Ref.
	US Specification (IEEE)		
IEEE 1609.2	IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages	2016, January	[63]
	EU Specifications (ETSI)		
TS 102 731	Intelligent Transport System (ITS); Security; Security Services and Architecture	V.1.1.1, 2010-09	[34]
TS 102 940	Intelligent Transport System (ITS); Security; ITS Communications security architecture and security management	V.2.1.1, 2021-07	[46]
TS 102 941	Intelligent Transport System (ITS); Trust and Privacy Management	V.2.1.1, 2021-10	[48]
TS 102 942	Intelligent Transport Systems (ITS); Security; Access Control Technical Specification	V.1.1.1, 2012-06	[36]
TS 102 943	Intelligent Transport Systems (ITS); Security; Confidentiality services	V.1.1.1, 2012-06	[37]
TS 103 097	Intelligent Transport Systems (ITS); Security; Security header and certificate formats	V.2.1.1, 2021-10	[47]

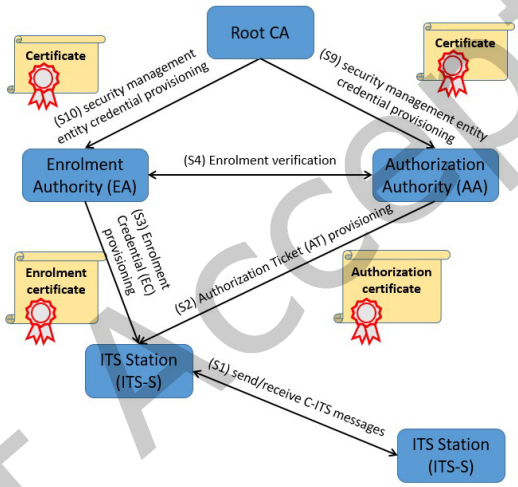

Fig. 3. Overview of Security Management System

Just Accepted

4.2 Differences between ETSI C-ITS and IEEE 1609.2

In this section, we describe differences in the security management systems between ETSI ITS and IEEE 1609.2 [63] (SCMS [17]).

4.2.1 Architectural Principles of Security Management. The SCMS architecture [17] ensures strong privacy protection of vehicle owners by enforcing strict separation of vehicle information and the network entities under different organizations. This architecture allows no single entity in the security management system to have access to information sufficient to identify a vehicle: identifying a vehicle in SCMS requires multiple management entities under different organizations to collude. To achieve this goal, this architecture includes purpose-specific entities such as Registration Authority (RA) and a pair of Linkage Authorities (LAs). This level of functional and ownership separation is beyond the extent of ETSI ITS certificate management system [46]. To achieve the

similar level of functional separation in ETSI ITS as in the SCMS, extra design and implementation steps are required beyond the scope of the ETSI ITS standard.

4.2.2 Revocation of ITS-S Certificates. The SCMS supports *active revocation* of pseudonym certificates. *Active revocation* means that the certificate management system revokes the pseudonym certificates of a vehicle by issuing a Certificate Revocation List (CRL). The SCMS defines separate entities dedicated for this task, such as Misbehaving Authority (MA) and a pair of LAs. When a vehicle observes misbehavior of another vehicle, the former reports to the MA by including the latter vehicle's *linkage value* which is included in its pseudonym certificate. Then the MA determines whether misbehavior exists or not by correlating multiple reports and verifying the alleged misbehavior.

Upon confirming the positive misbehavior, the MA resolves the reported *linkage value* to two *linkage seeds* by contacting the Pseudonym CA (PCA), the RA, and the LAs. The MA contacts these three entities in a serial manner in this process as each entity has only limited information that collectively triggers the LAs to retrieve the correct *linkage seeds* of the to-be-revoked vehicle.

After the *linkage seeds* are obtained from the LAs, the MA creates an entry in the CRL by including the tuple of (*linkage seeds*, current time period, and the number of simultaneously active pseudonyms). As vehicles receive the CRL, they use this tuple and reconstruct a set of *linkage values* that correspond to all pseudonym certificates of the revoked vehicle. This way, vehicles can identify revoked certificates by comparing the *linkage value* within the certificate in the received messages against the values reconstructed out of the CRL. This way, the number of simultaneously valid certificates or future certificates preloaded to vehicles does not impact the CRL size (cf. Sec. 7.3). We refer the reader to [17] for further details.

ETSI ITS does not define *active revocation* of certificates. Instead, it solely relies on a *passive revocation* mechanism. *Passive revocation* is accomplished by denying further allocation of certificates to a vehicle when the system determines that the vehicle needs to be revoked. This rejection occurs at the time when the vehicle attempts to obtain additional pseudonyms from the certificate management system.

4.2.3 Certificate Issuing and Usage Schemes. Annex 2 in the 5GCAR D4.1 document [56] describes the security architecture of the US and the EU certificate management systems. In the US system, the certificate management system (more specifically the RA and PCA collectively) generates three-years worth of certificates and preload them to a vehicle, containing 20 pseudonym certificates per week to a vehicle [17, 56]. This pseudonym size is derived from C2C-CC recommendation [15] as stated in SCMS [17].

An ETSI report on pseudonym change management in TR 103 415 [43] lists six different types of pseudonym management schemes. Given the nature of a pre-standard report, it does not yet specify exact details in this area. It indicates that the pseudonym pool size in referenced schemes varies between 10 to 100 depending on the scheme. The underlying mechanism is that a vehicle cycles through a set of certificates for a fixed duration of a week. The smallest size of 10 is the proposal from SCOOP@F project [103] and the largest pool size of 100 is the recommendation by EC's security policy and governance frame work [23] and certificate policy [24]. One exception is Issue First Activate Later (IFAL) scheme [110] which strictly uses only one pseudonym at a time without reuse.

Neither the aforementioned 5GCAR D4.1 document [56], SCMS [17], nor the ETSI ITS specifications [46, 48] explicitly specify the change period of one certificate from another within a one-week period. This period influences a vehicle's vulnerability to tracking and identification. Multiple schemes may be employed for this purpose; this period may be static for all vehicle types under all circumstances, or may vary depend on vehicle types and specific circumstances.

Just Accepted

5 ATTACK TYPES AND THREATS

Before we discuss individual security and privacy-related issues in the subsequent sections, we first identify attack types and their resulting threats. Table 2 captures our view on this point. This table is not intended to be exhaustive; in fact, there may be new types of attacks we are not aware of today but become possible in the future. However, it is important to be cognizant to this important aspect.

Table 2. Attack Types and Threats

Attack types	Attack Description	Resulting Threats
Passive vs. *Active*	*Passive*: monitor communication channels and obtain information from it. *Active*: send disruptive messages to the communication channels or breaks in a system.	*Passive*: collected data can identify or trace vehicles. *Active*: disruptive messages may cause accidents, or intrude the system resulting in information loss or system malfunction.
Local vs. *Remote* scope	*Local*: passively monitor or actively send disruptive messages at a specific location to its immediate area. *Remote*: passively monitor or actively send disruptive messages to/from one or more remote locations.	*Local*: the scope and impact of data collection and disruptive messages is limited to a specific area only. *Remote*: the scope and impact of data collection and disruptive messages spans farther to wider areas.
Local vs. *Global view*	*Local view*: data collection in a limited scope, e.g. using a single or small number of devices in a limited area. *Global view*: data collection and aggregation from large number of devices in a wide area.	*Local view*: obtains traffic flow or pattern within a limited area. *Global view*: obtains traffic flow or pattern in a wide area, such as entire country.
Insider vs. *Outsider*	*Insider*: an employee of RSU infrastructure system steals data or disrupts its operation. *Outsider*: a hacker builds a device that sends messages as a fake vehicle, or breaks in a system.	*Insider*: loss or leak of data that are otherwise available only to insiders. *Outsider*: disruptive messages from a fake device cause negative consequence such as accidents.
Individual vs. *Organized*	*Individual*: a motivated hacker with limited budget and materials with an intent to disrupt communication. *Organized*: an organized group (e.g. nation state) with unlimited resources with large budgets, facilities, and materials with intentions to disrupt an enemy nation.	*Individual*: limited impact relative to the effect a single individual can cause, e.g. a small number of fake devices. *Organized*: more organized and larger-scale attacks possible using a dedicated infrastructure.

Just Accepted

Different types of adversaries have different motivations and goals. An individual hacker may have fun out of disrupting society, and would likely be satisfied to see the resulting chaos in reality. On the other hand, a large organized crime group may aim to disrupt peace in an enemy nation with an intention to cause chaos, physical and material damages, and panic. In both cases, adversaries' motivations and goals are related to the aspects of the CIA triad [26].

- Reduced confidentiality: as a result of compromising privacy of vehicle owners by tracking and identifying vehicles.
- Reduced system integrity: by making it untrustworthy, e.g. by introducing fake vehicles injecting false messages.
- Reduced system availability: by disrupting the objective to promote road safety, such as by creating denial-of-service (DoS) situation.

6 SECURITY ISSUE: PRIVACY PROTECTION

One of the goals of the security management system in V2X communication is privacy protection, i.e. protecting the vehicle owners' privacy as required by relevant regulations. In the EU, these are GDPR [95], Network and Information System (NIS) Directive [29], the Cybersecurity Act [6], and the ePrivacy Directive [91]. Thus, user privacy protection is a requirement for V2X communications. Privacy protection technologies aim to prevent attacks or to confuse attackers who attempt to track vehicles by intercepting communications or tracing V2X interactions. A range of privacy protection strategies have already been developed and partially standardized. It is important to ensure that these privacy-preserving approaches do not impede safety functions which rely on vehicular communications.

A key strategy to achieve privacy protection is to rely on periodically changing pseudonyms for all communication involving vehicles. To provide pseudonyms to vehicles, certificate management systems such as SCMS [17] have been designed for the US based on PKI [7] (cf. Sec. 4.2.3). The EU security architecture is based on the same approach. Privacy protection includes the following concepts as defined by Pfitzmann and Hansen [93]:

- Anonymity: *"Anonymity of a subject means that the subject is not identifiable within a set of subjects, the anonymity set."*
- Pseudonymity: *"Pseudonymity is the use of pseudonyms as identifiers"*
- Unlinkability: *"Unlinkability of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these IOIs are related or not."*
- Unobservability: *"Unobservability of an item of interest (IOI) means (i) undetectability of the IOI against all subjects uninvolved in it and (ii) anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI."*

Protecting the vehicle owners' privacy is a meaningful goal. However, there are several scenarios worth considering for the applicability of privacy protection. They appear to directly conflict with the privacy protection requirement.

6.1 Privacy and Vehicle Operation

Vehicles with no malicious intent store certificates from other vehicles as a part of their normal operation. How long vehicles store these certificates have implications on privacy of vehicle owners. Vehicles store other vehicles' certificates for several reasons. First, verification of sender's authenticity requires verifying the entire certificate chain from up to the RCA. However, messages may not necessarily contain all certificates in the chain. Therefore, once a vehicle obtains the entire certificate chain for a given AT, it needs to keep this set for future references. Second, some message types (i.e. CAM, cf. Sec. 6.4) do not always contain an AT in every message. This implies that receiving vehicles need to store a copy of this AT to verify the message integrity as long as the transmitting vehicle uses the said AT. Therefore, the difference between malicious and benign devices are subtle: presence or absence of malicious intent to use collected information. In this sense, privacy protection implicitly includes protection against benign vehicles also. We consider this is a fundamental constraint of the certificate-based message verification in broadcast-mode. This point raises a question: when does a benign vehicle deletes *old and stale* ATs that has been stored in it but no longer used due to, either the AT-owner vehicles changed their ATs, or they moved out of the communication range from the vehicle. Another question is a requirement to retain received ATs for forensics purposes, such as investigating accidents. If such requirement exists, it may vary in countries or jurisdictions, thus likely not a one-size-fits-all answer. In this respect, these questions are implementation-dependent matter. Differences in these aspects likely influence the privacy of vehicle owners as how long privacy-related information is stored in other vehicles. The ETSI standard does not address either of these questions, leaving as an open issue in the standard.

Just Accepted

6.2 Applicability of Privacy 1: Vehicle Types and Usages

There are multiple types of vehicles on the road, and the privacy requirements are not likely to be applied to all of them uniformly. ETSI TS 102 941 [48] specifies the privacy requirements for ITS. However, it does not consider the option to apply different privacy measures depending on the vehicle type.

First, not all vehicles are privately owned. Some special vehicles and non-passenger vehicles are owned by a company rather than by an individual. Trucks, delivery vans, and taxis fall into this category. These vehicles quite often have a company name or a logo written on the vehicle's body. Even a privately-owned vehicles may have a name, an address, an email address, and a telephone number written on the vehicle's body if its owner has a private business to advertise. In this sense, many vehicles voluntarily forfeit the privacy information. Although drivers or vehicle owners wish to protect their privacy, it is an imbalance between volunteering visible information and a need to prevent *remote* tracking. Second, some special vehicles, such as police cars, ambulances, and public transportation (e.g. buses), belong to various levels of government or public entities rather than an individual. Hence, in this case, different level of privacy protection may apply for these vehicles while considering their minimum level of protection against tracking.

According to ETSI TS 102 941 [48], OEMs are expected to assign a canonical permanent vehicle ID to each vehicle at the time of manufacturing. This permanent ID is what the privacy protection requirement intends to protect by using pseudonyms instead. However, OEMs do not know for what purpose any given vehicle will be used at the time of manufacturing. For example, for the exact same type vehicles, one of them may be used by an individual owner; another may be used by a business to which no particular individual is associated with. The former case requires more strict privacy protection than the latter. Therefore, it is likely that we need to rely on other mechanisms to determine what level of privacy a given vehicle requires. This type of consideration is not given in the ETSI ITS specifications.

Another related aspect is the change of vehicle ownership. When a vehicle is sold in the second market, the privacy-related information of the previous owner stored in the vehicle needs to be erased. This includes data such as unused ATs, navigation history, and Bluetooth-paired smartphone. The sales process of second-hand vehicles needs to include the necessary procedure to erase these data. As vehicles can be sold by owners rather than by auto dealers, it should be a simple process to trigger it through vehicle's user interface (UI).

6.3 Applicability of Privacy 2: Non-Vehicle ITS-S

There are different types of ITS-S, most prominently the vehicles, and the road-side RSU. ETSI ITS TS 102 940 [46] describes the overall certificate management system. However; the standard [46] only considers a vehicle-centric view of the system; it has no description on the certificate management for RSUs as another type of ITS-S.

As discussed in Sec. 6.2, privacy requirements are intended to protect the privacy of vehicle owners as private individuals. However, RSUs do not have any private owner or person associated with it. Therefore, it follows that RSUs do not need pseudonyms. The fact that privacy requirements may depend on the ITS-S type is not considered in the ETSI ITS specifications. How pseudonym certificates are managed for RSUs, or whether they are necessary for RSU at all, is not specified. See the related discussion in Sec. 7.5.

6.4 Privacy and Cooperative Awareness

Cooperative Awareness Messages (CAM), as specified in ETSI TS 302.637-2 [44], share basic attributes of the vehicles on the road. These attributes include the vehicle's position, speed, direction, acceleration, vehicle length and width, vehicle type, etc. Vehicles on the road periodically transmit CAM messages to mutually establish and maintain situational awareness in the vicinity. At the same time, vehicles change their pseudonyms periodically to preserve privacy and prevent tracking, as specified by EN 302 636-6-1 [40]. They also need to change their MAC address at the same time (and its IPv6 address in case of IP-based communication). This simultaneous

Just Accepted

changes of pseudonym, MAC and IPv6 address prevents adversaries and other vehicles from linking consecutive pseudonyms by either the MAC or IPv6 address.

Despite this privacy-protection scheme, broadcasting vehicle information in CAM can reveal sufficient information for receiving vehicles to identify the transmitting vehicle. For example, if there are only a few vehicles in the distinctive positions relative to the receiving vehicle (e.g. one in front and another behind), then the receiving vehicle can correlate the CAM messages with the vehicle by comparing the received position information against its own position. In another example, if a received CAM message indicates the transmitting vehicle is 15-meter long and there is only one 18-wheeler truck in the vicinity, it is also trivial to correlate this message to that vehicle. In fact, study by Escher et al. [32] found that additional information such as vehicle size *"enormously improves"* the pseudonym linkage, allowing tracking of up to 80% of vehicles. Further, the number of vehicles in the vicinity plays an important factor. This study concludes that the location privacy will decrease despite the change of pseudonyms.

Further, if vehicles collect and store pseudonym changes from vehicles based on relative position information, share and collaborate this information in a wider-scale, for example by uploading it in a cloud storage, real-time tracking of vehicle movement, such as city-wide level or even larger scale, would become possible. This way, vehicle tracking may become similar to what already exists in real-time flight and ship tracking maps such as in [54, 77].

In this way, simply transmitting CAM messages including position information and other attributes already helps a receiving vehicle to identify the transmitting vehicle, which leads to a possible compromise of the privacy of the vehicle owner. ETSI TS 102 940 [46] Clause 4.3.1.3 states: *"... it is necessary to ensure that the data cannot be linked to any individual so that no personally identifying information is leaked by the CAM service."* If we take this requirement text literally, the CAM message itself does not reveal the personally identifying information. However, the content in the CAM message provides information that certainly helps to violate the principle of privacy protection by linking the transmitted message and the vehicle that transmitted it.

One possible approach to mitigate this situation is to enforce strict one-time use of pseudonym. However, it still does not guarantee the unlinkability property if series of pseudonym changes are observed by and shared with multiple vehicles through the cloud storage. This approach also increases the required number of pseudonyms per vehicle; it will stress the management system to generate and deliver pseudonyms and vehicles to store them. The pseudonym change scheme as specified in standards requires further research.

6.5 Privacy vs. Road Safety

Privacy protection is at odds with road safety. Consider a simple scenario where there are multiple vehicles in a multi-lane road as shown in Figure 4. Vehicle A suddenly applied a brake which triggers the broadcast of an emergency electronic brake light (EEBL) message to the surrounding vehicles. The EEBL message is one of the De-centralized Environmental Notification Messages (DENM) as defined in ETSI TS 302.637-3 [45]. In this case, Vehicle B, which is directly behind Vehicle A, needs to brake immediately to avoid an imminent collision. This is an essential requirement to reduce the number of road accidents. However, due to the privacy requirements, TS 102 940 [46] states that the pseudonym used in DENM must be different (unlinkable) from the one used in CAM. This way, the message origin of the EEBL is kept anonymous and unobservable, meaning that Vehicle B is neither expected to know which vehicle originated this EEBL message, nor can it determine whether a specific vehicle (e.g. Vehicle A) transmitted this message or not. Therefore, it follows that all vehicles not only cannot determine whether to apply its brake or not, but also making a wrong decision can make the situation even more dangerous, e.g. Vehicle D or G applying a sudden braking for no apparent reason. At the same time, all DENM messages, including EEBL, include position information of the transmitting vehicle according to the specification in ETSI TS 302 637-03 [45]. This is a contradiction to the privacy requirement (cf. Sec. 6.4).

Just Accepted

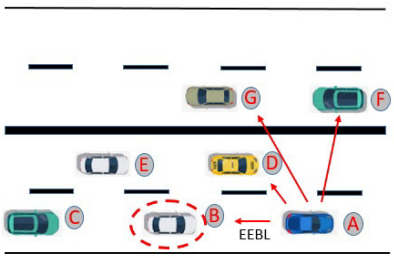

Fig. 4. DENM and Privacy Requirement

This simple example illustrated above indicates that the privacy protection requirement is directly at odds with road safety. This leads to several issues:

- The privacy protection requirement hinders other vehicles to identify where a message comes from.
- Lack of this knowledge hinders surrounding vehicles to make right decisions to prevent an accident.

The analysis by Chator and Green [21] also identified these points in the security requirement in the ETSI ITS specifications; we agree with this analysis. Based on the discussion above, we conclude that the privacy requirement in ETSI ITS specifications needs to be reconsidered.

6.6 Privacy and Use of Unicast

Some use cases in the EU projects [5, 19, 20, 25, 27] are based on unicast communication between two endpoints. Some examples include remote driving or tele-operated driving use cases in the 5GCAR [52] and 5G CroCo project [92]. Unicast communication has an advantage over broadcast in that the former can use confidentiality protection through encryption. This prevents passive observers from identifying the information transmitted by a vehicle. Although there are methods to apply confidentiality protection in broadcast, such as those proposed in [30, 57, 59, 99], the ITS specification (TS 102 943 [37]) does not require it to broadcast-based services such as CAM and DENM.

Despite the use of confidentiality protection, unicast communication conflicts with the privacy requirement. This applies to both internal and external threats. The internal threat refers to the leakage of private information between two endpoints of the communication; the external threat refers to the leakage of private information to another entity outside of these two endpoints.

First, we discuss the internal threat. If two entities establish a unicast communication, then by definition, both of them uniquely identify the other endpoint with the pseudonym, IP or MAC address of the other endpoint. In this case, applying a periodic pseudonym change is meaningful to protect the communication from eavesdroppers (i.e. protection against external threat). It makes it difficult for them to track unicast communication over a period longer than the pseudonym change cycle. However, it also means that the *linkability* of the old and the new pseudonym is voluntarily shared with the peer endpoint of the unicast communication. The peer vehicle can keep this information even after the unicast communication ends until the time that the vehicle changes its pseudonym again later. In addition, changing pseudonyms in the middle of unicast communication requires an explicit coordination between the two endpoints to maintain the communication. If this procedure fails for any reason, it can result in a negative consequence, such as a dropped communication.

The change of pseudonyms in unicast communication requires special handling, similar to Network Mobility (NEMO) in RFC 3963 [28]. It operates at the IP layer as described in ETSI EN 302 636-6-1 [40]. Therefore, an additional mechanism is needed to handle link layer address changes. 3GPP TR 33.836 [3] defines several variations of such explicit link layer address change notification. These schemes are workable solutions. However,

Just Accepted

as stated earlier, they fundamentally violate the *unlinkability* requirement between two endpoints in exchange for maintaining the unicast communication.

Second, from an external threat perspective, pseudonym changes in the ongoing unicast communication require confidentiality protection. Otherwise, it would be trivial for eavesdroppers to intercept the pseudonym change messages sent in clear and correlate the pseudonyms, hence violating the *unlinkability* requirement.

Another possible approach is simply avoiding the pseudonym change until the unicast communication is completed. This is especially meaningful if confidentiality protection is not applied. In this case, both vehicles can change their pseudonyms as soon as the unicast communication ends. Doing so ensures that the *unlinkability* principle is maintained. This approach is also beneficial as it eliminates potential failure of pseudonym change and communication loss in the middle of unicast communication. Further consideration is needed to ensure reliable unicast communication while satisfying the privacy requirement.

7 SECURITY ISSUE: USE OF CERTIFICATES

Both the EU and the US systems are based on Public Key Infrastructure (PKI) [7] and use of certificates to manage the pseudonym usage. In this section, we focus specifically on aspects related to their usage. We will cover the actual issues and lack of definitions in the two competing standards (ITS-G5 and C-ITS) impacting certificate usage, renewal and revocation concerning vehicles, roadside infrastructures as well as pedestrians.

7.1 Certificate-Based Message Verification

In V2X communication, a certificate is attached to a message and receivers of this message use the public key in the certificate to verify the message's authenticity. The PKI in charge of managing certificates [7] requires that the receiving entity should be able to verify the certificate chain up to the root CA in order to verify the message authenticity. This is the underlying assumption of using certificates in real-time communication.

Contrary to this assumption, the real-time verification of the certificate may not be possible under all circumstances. It is especially the case in a dynamically changing communication environment involving moving vehicles in open space. For example, CAM messages do not always contain a certificate. CAM messages contain a certificate at least once a second. However, when they are sent more frequently, a *digest* (the least significant 8 octets of a hash output of a certificate) is added to replace a certificate. This use of *digest* enables a compact representation of a certificate without sending it in every CAM message. TS 103 097 [47] states that, if a vehicle receives a CAM message with unknown digest or a received certificate is signed by an unknown AA, then the receiving vehicle needs to resolve this situation by requesting the missing certificate to the surrounding vehicles and wait for a response (*inlineP2pcdRequest*). Only after this step, the vehicle can verify the validity of the received message. This additional message exchange causes delay in message verification in the order of several 100 milliseconds at least. This situation contradicts with the underlying expectation to process vehicular communication in real-time under all circumstances. Due to these issues, message identification based on certificate verification as a mean to ensure authentication in V2X communications remains an open issue.

7.2 Certificate Usage and Change Policy

As discussed in Sec. 4.2.3, the certificate management in the EU issues a set of ATs per week [56]. ATs used in the V2X communication are expected to be changed periodically in the order of minutes. This implies that a set of ATs are reused multiple times during a specific one-week period. However, the exact duration of one AT and the mechanism to select the next one is not specified according to ETSI TR 103 415 [43]. If ETSI standard stops at the level of recommendations and leave details to implementations, there will likely be variations in terms of its effectiveness in preventing adversaries from predicting the next AT. In this sense, careful considerations are required as sub-optimal usage and change policy can lead to successful linking of the certificate to the vehicle.

Just Accepted

We also discussed the open issue of pseudonym usage and its implications on privacy protection in Sec. 6.4. Thus, it is an area that needs further consideration.

7.3 Certificate Reloading

Another area not specifically defined in the standard is the reloading of certificates. Under any circumstances, situations need to be avoided where a vehicle runs out of valid certificates, preventing that vehicle from sending messages altogether. Several research papers discuss certificate reloading schemes such as in [94]. These schemes use an RSU as an entry point to communicate with the AA. In these schemes, the underlying assumption is that an RSU is available whenever and wherever it is needed. However, RSUs may not necessarily be ubiquitous. Therefore, a universally workable solution is necessary so that legitimate vehicles can obtain new set of certificates without relying on the presence of RSU.

One possible approach is to store sets of certificates beyond the immediate period. Storing 3-years worth of certificates up front, as described in SCMS [17] and the 5GCAR D4.1 document [56], is one such approach. Such scheme, at least in theory, alleviates the reloading needs for the duration of three years. However, it comes at the expense of additional storage to hold this amount of certificates in the vehicle. Also, longer term storage of certificates complicates the system if they need to be revoked due to, for example, the vehicle being identified as malicious, or adversaries steal valid certificates from a legitimate vehicle and use them for malicious purposes. Another consideration is handling of unused certificates when the vehicle is deregistered, or when the ownership is transferred to someone else.

Another possible approach is to reload certificates for multiple periods in the future, or request the next set of certificates well before the currently stored sets are exhausted – analogous to refilling the gas tank well before it is empty. For example, a vehicle stores sets of n consecutive weeks worth of certificates, and requests the next sets well before the end of the n-th week. This approach gives extra time in case network connection is not available at the first attempt to contact the AA. In this case, the vehicle can retry within the remaining time. This approach avoids potential exhaustion of certificates at the end of every one-week cycle, and does not require large storage capacity compared to storing 3-years worth of certificates. As of today, the challenge to propose a system ensuring a continuous flow of valid certificates while contextually relevant and memory efficient for V2X message verification remains open.

7.4 Certificate Revocation

7.4.1 Active Revocation. Active revocation of certificates is an area that is distinctively different between the US and the EU systems as previously discussed in Sec. 4.2.2. The US system based on IEEE 1609.2 [63] (SCMS [17]) supports active revocation of certificates while ETSI ITS does not. Active revocation involves two aspects: 1) detection, reporting, and validation of vehicle misbehaviour, and 2) generation and distribution of the CRL. As the first aspect relative to handling misbehaviours is discussed later in this paper, in this subsection we focus on the latter – CRL generation and distribution.

Management of the CRL, including its generation and distribution, is already challenging in a conventional PKI-based system [106]. Notable difficulties are guaranteeing the distribution of the CRL in a timely manner and keeping up with the scale of the distribution itself. It is even more challenging with moving vehicles. Because vehicles are assigned with a set of certificates valid for a limited period as discussed in Sec. 7.2, the number of certificates per vehicle significantly impacts the CRL size. This situation requires a technique to aggregate current and future certificates that belong to a vehicle and represent them in a compact manner for efficient distribution. The situation becomes even more prominent if a large sets of certificates are preloaded to the vehicle ahead of time, as discussed in Sec. 7.3. We previously explained in Sec. 4.2.2 that in order to address this issue, the SCMS describes the revocation scheme using *linkage value*. It addresses one aspect of the distribution issues by

Just Accepted

reducing the amount of revocation-related information per vehicle. However, the CRL size is still a concern as the number of revoked vehicles increases over time. SCMS [17] does not address this aspect; it is most likely left as a deployment-level matter as it depends on the size of the vehicle population under a certificate management system.

Other issues of the revocation process remain open, especially the ones related to efficiently distributing the CRL. The main question on this issue is how to ensure the latest CRL is made available to vehicles in a timely manner. Even if the latest most up-to-date CRL is generated correctly, if it is not delivered to vehicles that need it when they need it, it is of little value. Online Certificate Status Protocol (OCSP) specified in RFC 6960 [101] is an alternative approach to the use of CRL. However, it does not solve the issue as OCSP suffers from the same issue of absence of guaranteed connection with the network under all circumstances [100].

The other related issue of CRLs distribution is their size versus the vehicle's storage capacity. Clearly, it is not realistic for a vehicle to store all revoked certificates of all vehicles. It is straightforward to consider that vehicles need to store CRL of vehicles that are *relevant* to them. By *relevant*, we mean related to vehicles that they may encounter on the road. There is no point of receiving and storing CRLs concerning vehicles that the receiving vehicle never comes across. However, how to determine the relevance is a matter of context for each individual vehicle. It depends on where a given vehicle drives, e.g. which country, region or province, highway or street, etc. Ideally, all vehicles that encounter a given revoked vehicle should be provided with the CRL containing the revoked certificates of that vehicle in question. If a vehicle misses a specific vehicle's certificates in its CRL and receives a message from this revoked vehicle, it does not know that it should reject all messages sent by this revoked vehicle. How to determine the relevance, or even the concept of CRL *relevance*, is not defined in IEEE 1609.2 [63] (SCMS [17]). Thus, it most likely falls in the implementation-dependent area. It is certainly not a trivial problem to solve, making it a possible further research area.

Previous research has been conducted on the subject of CRL distribution in V2X context proposing various schemes to make it efficient. Some of these schemes include: 1) splitting CRL in small pieces [68, 87], 2) distribution through RSU [90], 3) CRL dissemination in epidemic fashion [71], 4) use of Bloom Filter to reduce the CRL size [96]. Although these works include novel approaches to increase efficiency of CRL distribution, they do not address the *relevance* aspect we discussed.

Another issue related to CRL distribution is how to determine expired entries and when to remove them to prevent the CRL size from growing indefinitely over time. Even if a vehicle is already de-commissioned and thus is no longer on the road, it does not necessarily mean that these entries can be removed from the CRL as it is necessary to prevent the situation where adversaries can steal valid certificates and corresponding private keys from such vehicle to pose as a legitimate vehicle. Although many research papers focus on the CRL distribution, there is little attention to this area. This is not a trivial question as it closely relates to the preloading and reloading of certificates (cf. Sec. 7.3), i.e. the longer the perloading and reloading period, the longer the entry needs to remain in the CRL. This is also an open question that the IEEE 1609.2 standard [63] needs to address.

7.4.2 Passive Revocation. As discussed in Sec. 4.2.2, the EU system does not require active revocation of certificates, thus relies solely on passive revocation. Passive revocation is a scheme based on a *blocklist*. A malicious or misbehaving vehicle is blocklisted. Thus, when a vehicle sends a request to reload certificates next time, the certificate management system denies the request if the requesting vehicle is on the *blocklist*.

One advantage of passive revocation is its simplicity as the certificate management system alleviates itself from the trouble of generating and distributing the CRL to vehicles. However, the disadvantage of relying only on passive revocation is the very nature of being passive. In other words, it leaves a time-gap between the time the system revokes a given vehicle and the time when the vehicle stops its communication. The latter occurs when either all certificates in the vehicle expires or it voluntarily stops communication as the result of rejection to request new certificates.

Just Accepted

For example, if a vehicle stores only one week worth of certificates, it likely requests the next set for the following one-week period sometime toward the end of the current period – the timing in which the request is rejected if the vehicle is blocklisted. In worst-case scenario, this time gap can be up to 7 days. During this period, the vehicle continues to use its certificates; other vehicles certainly accept messages from this vehicle as valid. If the certificate reloading cycle becomes longer as the vehicle reload multiple weeks worth of certificates at a time, this time gap extends proportionally. Worse still, if the vehicle is preloaded with certificates for an extended period, such as 3 years, it does not request reloading for 3 years. This implies that certificate preloading for an extensive period is mutually exclusive with passive revocation approach. This way, the simplicity of the scheme comes at a price. ETSI ITS specification does not address this issue, thus requires further consideration.

7.5 Certificate Management of RSUs

As discussed in Sec. 6.3, RSUs do not require privacy protection and thus does not require the use of pseudonyms, strictly speaking. However, the certificate management system described in ETSI TS 102 940 [46] does not address these types of ITS-S or if any specific certificate management different from privately owned vehicles is required at all. This is another open area that needs to be addressed in the standards.

It may be necessary for vehicles to uniquely identify a specific RSU from another while still maintaining its anonymity. One possible approach is to assign pseudonyms with longer validity periods than those for vehicles, such as days, weeks, or months depending on how static the RSU pseudonyms can be. The similar principle may apply to non-privately-owned vehicles such as emergency vehicles. On the other hand, longer validity period negatively impacts revocation of such ITS-S types. For example, if an adversary hacks an RSU, steals its pseudonym certificates and corresponding private keys, and uses them on a fake RSU, this fake device can send legitimate messages for longer period than privately-owned vehicles. This situation is further pronounced in EU systems where it relies solely on *passive revocation*. Therefore, a good balance needs to be achieved in order to minimize negative impacts from such situations.

7.6 Certificate Management of VRUs

The EU projects related to V2X communication define various use case scenarios [52, 79, 84, 92, 111]. These projects are under 5G-PPP, thus their technology focus is naturally on C-V2X as opposed to ITS-G5. Many of the use cases captured in these documents involve new and unique aspects in C-V2X compared to ITS-G5. One example is Vulnerable Road Users (VRU). VRU refers to pedestrians, cyclists, other human or non-human road users [49]. Inclusion of scenarios involving VRUs extends vehicular communication and contributes to further improvement of the road safety. In 2010, ETSI EN 302 665 [33] defined handheld devices, or *personal ITS-S*, as one of the ITS-S types. However, subsequent ETSI specifications focused exclusively on vehicle-centric view only. In this respect, increasing interest of VRUs due to the emergence of C-V2X was the trigger to start standardization work specific to VRUs. In fact, between 2019 and 2021, ETSI published TR 103 300-1 [49], TS 103 300-2 [50], and TS 103 300-3 [51] which exclusively address VRU-related use cases, define functional architecture, and specify VRU basic service, respectively. The second specification [50] covers security-related issues. However, its content stays at the analysis level and leaves many issues open. The last one [51] specifies VRU Awareness Messages (VAM). It covers security aspects. However, the extent of its scope is limited; it does not define mechanisms and procedures such as enrolment of VRU devices and VRU-specific certificate policy including provisioning and usage of pseudonym certificates. In fact, it states that these areas are outside the scope of this specification (cf. clause 6.5.4 in [51]).

The above situation also means that the VRUs (handheld devices) as a type of ITS-S were not originally envisioned as a part of the certificate management system defined in ETSI TS 102 940 [46], and it is still the case today. In fact, we have already pointed out in Sec. 6.3 that the existing management system [46] is strictly

Just Accepted

vehicle-centric view only. This situation raises several points: 1) inclusion of VRU as a type of ITS-S, including certificate management of VRUs, 2) definition of a certificate management back-end system for VRUs, equivalent for vehicles as in clause 7 in [46].

Including the VRU as a type of ITS-S has several implications. VRUs use smartphones to communicate with other ITS-S, such as indicating pedestrians' presence to nearby vehicles. This obviously means that smartphones, as a type of ITS-S, need to become legitimate members in the V2X communication system, including provisioning and usage of pseudonym certificates as in vehicle ITS-S. Because the coupling between a human user and his or her smartphone is even tighter than that of vehicles, even higher level of privacy protection is required for VRUs. In addition, if a specific VRU device needs to be revoked for any reason, appropriate mechanism needs to be in place to ensure that it is excluded from the V2X communication. Introduction of smartphones can serve as an easily-accessible potential new attack surface to the whole V2X communication system. As these consumer products are readily accessible than vehicle OBUs, the threshold is lower for adversaries to develop a malicious software on an open-source-based OS (e.g. Android) using available open-source software development tools – picking up a smartphone and plugging in a USB cable to it is far easier and trivial than opening a part of a vehicle's dashboard, exposing a connection to the CAN bus and connecting to it. Hacking a vehicle OBU requires extensive knowledge, both mechanical and electronical, of vehicle's construction. In this sense, the above-mentioned VRU-specific specifications [49–51] fall short from addressing these aspects, leaving them as open issues.

One possible approach is to define a distinct ITS management system for smartphones separate from vehicles and RSUs. Separately manage smartphones likely simplifies the certificate management by isolating specific characteristics and aspects unique to them. One such example is the potential needs to interact with Mobile Network Operators (MNOs) if verification of the subscriber information is required before admitting the device as a legitimate member of the ITS system. At the same time, this separation of management also implies that an interconnection is needed between these two types of ITS-S management systems. In addition, multiple MNOs may be involved to accommodate subscribers of different MNOs, including MNOs of other countries to address roaming scenarios.

7.7 Certificate Usage in Multiple Communications

It is likely that vehicles are engaged in multiple different types of communication with different entities for different purposes simultaneously. For example, a group of trucks in a platoon communicates with one another to coordinate their movement while maintaining safe driving distance with adjacent trucks within the platoon. In this case, these trucks likely use either unicast or multicast (groupcast) mode of communication rather than broadcast mode. At the same time, these trucks also broadcast basic service messages such as CAM to other surrounding non-platoon vehicles. The intended target and purposes of these messages are different.

In this case, it makes sense to use different pseudonyms for different purposes. This approach also aligns with the privacy protection perspective as one pseudonym used for broadcast mode does not reveal the pseudonym used for unicast mode. This way of pseudonym separation is likely to be beneficial, especially because broadcast mode does not provide confidentiality protection from observers (cf. Sec. 8.1). Such separation of pseudonym usage enhances the security of V2X communication.

ETSI specifications EN 302 636-1 [38], EN 302 636-3 [39], EN 302 636-4-1 [42], EN 302 636-6-1 [40] discuss the use of multicast in GeoNetworking. They discuss security-related functionalities, such as authentication, authorization, integrity, privacy, and non-repudiation. However, they do not mention confidentiality especially in the context of user-plane traffic. Thus, encryption is not applied in multicast mode user traffic in GeoNetworking. Therefore, the vulnerabilities of multicast and broadcast traffic are at the same level. On the other hand, separate use of pseudonyms in unicast has a value as it can apply encryption, thus worth exploring this

Just Accepted

usage (cf. Sec. 8.2.1). However, it is not specified in these GeoNetworking related specifications and other key security-related specifications, such as TS 102 637-1 [35], TS 102 940 [46], or TS 102 941 [48]. As such, it embodies an interesting open challenge.

8 SECURITY ISSUE: COMMUNICATION MODES

8.1 Broadcast-Oriented Communication

The basic services provided by V2X communication includes CAM and DENM as defined in ETSI TS 302.637-2 [44] and TS 302.637-3 [45], respectively. These messages are broadcast to the surrounding vehicles. Broadcast messages, by definition, are sent to any and all entities within the communication range. This is in contrast to unicast or multicast messages, which are sent to a specific endpoint or a known group of endpoints. The very nature of the broadcast is that the transmitting node is not concerned with the number of receiving entities within the communication range and their identities. It is further aggravated with the dynamic topology changes due to moving vehicles. Therefore, a set of vehicles within a communication range of a vehicle are in the constant flux depending on the density and the relative speed differences. Another characteristic of broadcast messages is the absence of confidentiality protection as specified in TS 102.943 [37]. Therefore, any entity with a suitable equipment can receive these messages.

These two points are significant from a V2X communication perspective because any passive observer with a suitable device can receive, collect, and analyse CAM and DENM messages. The receiving entity can verify the message authenticity and integrity by using the certificate contained in the message itself. Due to the use of periodically-changing pseudonyms and the unlinkability property from the privacy protection requirement, it is not trivial to identify the transmitting vehicle. However, a passive observer can still detect and recognize the existence of a specific pseudonym in the vicinity just by observing messages. This way, the broadcast nature of the basic messages has no or little protection from persistent observers to collect messages and detect long-term patterns of any given vehicle. This is an area of concern from a privacy protection perspective.

8.2 Unicast – Confidentiality Protection

8.2.1 Applicability of Confidential Protection. Confidentiality protection applies to unicast mode only. On the other hand, basic services are based on broadcast mode as discussed in Sec. 8.1. This is captured in Table 2 in ETSI TR 102 893 [41]. Unicast-based communication is rather a minority in V2X communication and is limited to specific use cases. In other words, confidentiality protection is applicable to a rather small portion of V2X communication where unicast is used. The 5GCAR D4.2 document in [55] expresses a concern of the sole reliance on the PKI system [7] for security and privacy of V2X communication. A proposed scheme in [55] introduces a new entity called *key manager* that generates symmetric keys for encryption. The proposed scheme is a step towards introducing an additional security mechanism. However, it overlooks the fact that the confidentiality protection is applicable to unicast mode only. Thus, it has limited applicability in V2X communication.

8.2.2 Usability of Unicast Communication. The use of unicast in V2X communication is likely an IP-based communication to support value-added services. ETSI TS 102 941 [48] states that the use of IPsec or TLS is assumed for the confidentiality protection in unicast. The use of IPsec or TLS implies a notion of a *session* between two endpoints. Security Association (SA) establishment involves a handshake procedure which is an important factor to consider in a V2X communication environment where the vehicle topology changes constantly and dynamically.

The same characteristic of dynamic topology change as discussed in Sec. 8.1 equally applies to unicast communication. The communication range of DSRC is expected to be 300 meters [16]. Then, depending on the relative speed and direction of vehicles, the communication between two ITS-Ss can be short-lived in the order of seconds. For example, if we assume communication between an RSU at a fixed location and a vehicle moving

Just Accepted

at 120 km per hour, the communication lasts only 9 seconds. In the case of vehicles moving in the same direction, the communication between them may last longer. For example, if the relative speed difference of two vehicles is 10 km/hour, then the period they are within the communication range is 108 seconds, assuming a 300-meter range. Obviously, as the relative speed difference increases, the time duration shortens proportionally. Whether this time period is meaningful to establish an SA between two vehicles or not depends on the use cases and scenarios in which unicast communication is used.

A prime example where the use of unicast makes sense is when one of the endpoints is a remote entity over the long-range communication (V2N), such as remote driving discussed in Sec. 6.6. In this case, the vehicle's location or speed is not a factor. However, this is a rather value-added use case beyond the basic service. Strictly in V2V scenarios, a group of trucks in a platoon is one example where unicast communication makes sense as they move in the same direction with short inter-vehicle distance for extended duration. However, in other situations of V2V or V2I communication, in the worst case, vehicles may go out of the communication range as soon as an SA is established, rendering SA establishment a moot point. It is worthwhile for the ETSI ITS specification to include a guidance on the usability of unicast in V2X communication.

9 SECURITY ISSUE: MESSAGE HANDLING

9.1 Plausibility Validation and Misbehavior Detection

The concept of plausibility is present in different security aspects of V2X communications as specified in ETSI TR 102 893 [41] and EN 302 636-4-1 [42]. The idea of validation via plausibility, and why it is necessary in vehicular communication, is intuitively clear. A receiving vehicle needs to detect and reject bogus messages transmitted by an entity with a malicious intent to cause an accident or a road hazard, or to reject faulty messages transmitted by a vehicle with malfunctioning sensors. In this sense, plausibility validation is one of the key countermeasures to prevent potential threats in vehicular communication. There are two distinctive elements in the plausibility validation: 1) plausibility determination, and 2) misbehavior detection.

9.1.1 Determination of Plausibility. ETSI TR 102 893 [41] clause 11.3.20 states: *"Plausibility checks are non-cryptographic measures which use rules and other mechanisms to determine the likelihood that received data is correct. These rules and mechanisms range from simple heuristics to quite sophisticated and more complex, methods."* Also, clause B.4.5.3.2 in ETSI TR 102 893 [41] describes suspicious behaviors as *"any behavior that does not comply to expected behavior, based on direct evidence and probabilistic models."* It lists examples such as spurious and bogus packets. A spurious packet contains a proper signature but flawed payload; a bogus message contains a flawed signature. These definitions in the standard describe the intent of what plausibility check aims to accomplish, but it lacks clarity in terms of what qualifies as a good or valid plausibility check. Plausibility in V2X communication revolves around the idea of determining whether a given received message from another entity is reasonably genuine and thus should be accepted as valid. This level of message validation is above and beyond the verification of message integrity using digital signature.

Judging the plausibility of received messages may involve a number of contextual factors, such as: 1) location, 2) vehicle's mobility (e.g. position, speed, and direction), 3) environment (e.g. local street or highway), 4) time of the day (e.g. rush hour or last night), and 5) other conditions (e.g. weather). However, these definitions in the standard are too abstract to be usable in reality to identify messages that do or do not conform to a given criterion. In other words, a more concrete and unambiguous definition is needed with respect to what constitute a set of criteria usable for plausibility validation. In addition, plausibility check needs to occur in real-time with high confidence to process time-critical messages such as DENM, which requires urgent and timely reaction such as an indication of an approaching emergency vehicle. In this sense, the result of plausibility validation determined too late or with less than 100 per cent confidence is either useless or may even result in an undesirable consequence.

Just Accepted

Not defining a set of criteria for plausibility validation implies that it is left up to individual implementations on how it is accomplished. Such situation will most likely results in variations of coverage and effectiveness among them, where some of them better secure operational abilities than others in practice. Clearly, such situation is undesirable. However, establishing such criteria has a number of benefits such as:

(1) Unambiguously defining how vehicles should behave under specific situations,
(2) Minimizing variation of implementations so that all vehicles on the road will have uniform and predictable behavior under the same situation,
(3) Enabling OEMs to evaluate their implementations during development cycle for validation and improvement,
(4) Raising consumer confidence for successful adoption of the V2X technology in the market.

While this is arguably a difficult area to standardize, possible definition of common criteria is worth pursuing in standards given the potential benefits. One possible approach is to define a common *minimum set* of criteria that all OEMs must comply in their implementations. It can be done by defining a set of scenarios, associated with expected plausibility judgement and behaviour by vehicles. If a given OEM chooses to enhance its implementation with additional scenarios, it can be a differentiator from other OEMs without affecting the standardized set of scenarios.

9.1.2 Misbehavior Detection. Misbehavior detection is closely related to plausibility validation. They are two sides of the same coin. Detecting misbehavior implies detecting and analyzing patterns of plausibility validation failures on messages from another entity over time. Most likely, a single plausibility failure does not constitute a positive misbehavior detection. It requires continuous evaluation over time to determine if a misbehavior condition exists or not to reach reasonable level of confidence. Studies by van der Heijden et al. [109] and Ambrosin et al. [9] provide good basis for various approaches toward misbehavior detection. Especially, the analysis in [109] captures a comprehensive overview and in-depth analysis of many misbehavior detection mechanisms. It analyzes and categorizes various mechanisms and classifies them into two dimensions, resulting in four categories.

The two dimensions described in [109] are: 1) *node-centric vs. data-centric*, and 2) *autonomous vs. collaborative*. The first dimension concerns with whether focusing on transmission patterns of a specific entity or analyzing data irrespective of the transmitting entity. The second dimension concerns with whether misbehavior detection is done locally within a node or as a result of exchanging information with other nodes. The resulting four categories are:

- *Behavioral* (*node-centric* and *autonomous*)
- *Trust-based* (*node-centric* and *collaborative*)
- *Plausibility* (*data-centric* and *autonomous*)
- *Consistency* (*data-centric* and *collaborative*)

Each of these four categories is based on certain conditions and assumptions. Thus, none of them is universally applicable under all circumstances. For example, *collaborative*-based models (i.e. *trust-based* and *consistency*) imply that there are multiple vehicles in the area with which a vehicle can exchange information with to make an assessment on a specific vehicle. If there is not sufficient number of vehicles in the immediate area or not enough data is available to reach a conclusion, mechanisms in these categories are not effective. Another aspect of *collaborative* category is the concept of *honest majority* – an assumption that the majority of the vehicles are honest and provide genuine information. However, if there is a small proportion of malicious entities or vehicles with faulty sensors providing incorrect data, it can skew the final decision on a vehicle in question.

The *autonomous*-based models (i.e. *behavioral* and *plausibility*) solely rely on data within a vehicle. Therefore, the assessment and the decision of whether a given vehicle is misbehaving or not is necessarily limited to the

Just Accepted

information within the vehicle. The vehicle may reach a different decision if it has information other vehicles may have but does not locally. In this respect, combinations of all 4 categories is likely necessary to cover all possible scenarios and to gain confidence in the misbehavior detection. This is another area that needs further study. Ideally, a single solution that covers all possible situations is desirable. So far, the analysis in [109] indicates this is not the case.

Similar to plausibility validation, misbehaviour detection will likely result in different levels of effectiveness if it is left up to implementations. Defining a common approach or common test set to evaluate different implementations is worthwhile to guarantee uniform detection of misbehaviour. As discussed in Sec. 9.1.1, the same approach to standardize a common criteria will be helpful to achieve the same benefits for misbehaviour detection.

9.2 Communication involving Vulnerable Road Users

As discussed in Sec. 7.6, emergence of C-V2X introduces new use cases involving VRUs. They relate to the safety of road users other than vehicles such as pedestrians and cyclists who uses smartphones as a type of ITS-S. VRU-related messages include communicating presence and movement of pedestrians or cyclists to vehicles, or vice-versa. TS 102 300-3 [51] specifies VAM; these messages enable VRU devices to communicate its position and movement with vehicles or other VRUs to improve road safety. Specifying these messages is a step forward to achieve this goal. However, this specification hints that more work is needed. Informative annex G in this specification gives a glimpse into unique issues and difficulties associated with VRU scenarios. It has to do with the unpredictable nature of pedestrian's movement compared to that of vehicles. One example is the transition from a pedestrian to a cyclist, and vice-versa, and how VAM messages accurately reflect this transition (e.g. VRU profile to change from a *pedestrian* to a *cyclist*). This annex indicates that these transitions are not a trivial problem to solve, thus requires further research and standardization.

10 SECURITY ISSUE: SYSTEM LEVEL ISSUES

10.1 ITS-S Device-Dependent Trust Level

ITS-S consists of different types of devices. Vehicles are manufactured by OEMs and a large proportion of them is owned and used by private individuals. On the other hand, RSUs are special type of devices owned and managed by government authorities, and they are installed at fixed locations on a permanent basis. In this sense, it may make sense to differentiate the level of trust for vehicles and RSUs. In other words, the trust level for RSUs can be higher than vehicles and treat messages differently based on the message source. It implies that receiving vehicles need to distinguish message sources, at a coarse level such as *RSU-type* or the *vehicle-type*. Such differentiation does not compromise the privacy requirement (anonymity property).

In addition, such device type-level identification has benefits. For example, trusting messages from RSUs may be useful in addressing new approaches in plausibility validation or misbehaviour detection discussed in Sec. 9.1. One possible approach to address misbehaviour detection is to have intelligence in RSUs to collect and analyse data sent by vehicles, and integrate data from other RSUs at the back-end system to detect positive misbehaviour of vehicles. Then, this information can be distributed to vehicles in the area as an *authoritative information*, which can only be sent by RSUs. A survey by Wang et al. [113] discusses this concept as one of the approaches of certificate revocation by considering RSUs as an Intermediate Authority (IA). The concept of *authoritative information* is somewhat akin to distributing CRL from the PKI system. The certificate definition in IEEE 1609.2 [63] includes `SubjectAssurance` which can fit for this purpose. However, it also states that the exact content definition is outside its scope. This is another area for further research.

A potential issue of this approach is an abuse of trust level if adversaries can compromise an RSU and modify its behaviour. However, protection against unauthorized tampering with malicious intent is a general issue that

Just Accepted

applies to all ITS-S types. Thus, it falls into the issue of hardening devices against such attacks. Specifically, TS 102 940 [46] recommends the use of HSM as a solution.

10.2 Interconnection between Multiple Security Management Systems

A vehicular communication system involves government authorities that manage RSUs embedded in traffic lights and other road infrastructure that communicates with vehicles. This system also manages certificates to vehicles as specified in ETSI TS 102 940 [46]. However, it is not just one management system, but multiple systems. A security management system most likely exists per appropriate geographical domain that has authority over specific jurisdiction. Depending on the deployment of the system, there may be one such management system at the national level, state or provincial level. It is up to individual country and its relevant authority to determine how this management system is owned and managed.

If we consider the certificate management system as described in ETSI TS 102 940 [46], each vehicle is expected to belong to one such management system. However, vehicles on the road likely belong to different such management systems. For example, highways in any given EU country are used by vehicles from multiple countries in addition to local vehicles. The above point implies that there needs to be an interaction between multiple management systems.

The following examples illustrate the relevant scenarios. As the first example using Fig. 5, we consider a scenario where a vehicle (V_{A1}) from Country A travels to Country B (event 1). During its stay in Country B, V_{A1} is involved in a minor accident that causes some of the sensors to malfunction. As a result, V_{A1} starts to report inaccurate or incorrect events and generates faulty messages to surrounding vehicles. In this case, a local vehicle (V_{B1}) in Country B determines a misbehavior condition of V_{A1} and reports this event to its certificate management system (MS_B) in Country B (event 2). However, certificates of V_{A1} were issued by the management system (MS_A) in Country A. Therefore, there is nothing MS_B can do unless there is an appropriate mechanism in place. It includes steps such as: 1) MS_B to identify the V_{A1}'s country of origin and to notify such event to MS_A (event 3), 2) MS_A to revoke V_{A1}'s certificates and report it back to MS_B (event 4).

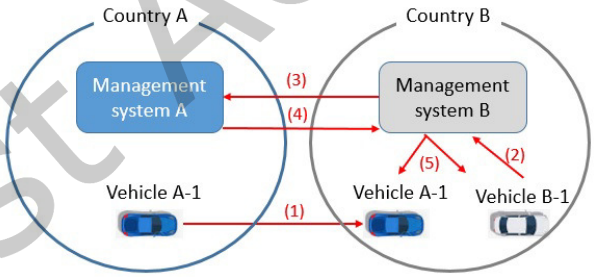

Fig. 5. Scenario of Interconnection between Management Systems

Another example is the active revocation of vehicles. This is applicable in the US system as discussed in Sec. 4.2.2. If the management system revokes a vehicle, it generates and distributes the CRL containing this vehicle's information. However, in this case, vehicles (V_{Bs}) that encounter this vehicle on the road in Country B also need to receive this CRL so that V_{Bs} can correctly disregard any messages sent by V_{A1}. For this scenario to work correctly, MS_B needs to be notified of the revocation condition of V_{A1} from MS_A so that MS_B can distribute the CRL to vehicles in its territory. These aspects involving interaction across multiple security management systems are not covered in the ETSI ITS specifications. Given that cross-border mobility is a daily normal events in Europe, ETSI needs to address these aspects.

Just Accepted

10.3 Multiple Security Management Systems for Different ITS-S Types

As discussed in Sec. 6.3, ITS-S consists of multiple different types (i.e. vehicles, RSUs). However, ETSI TS 102 940 [46] does not clearly specify how these different ITS-S types should be managed in the most effective and meaningful manner. Because these two types of ITS-S are owned and are used differently, it may make sense to manage them under separate management systems. For example, RSUs are owned, administered, and managed by government authorities, while majority of vehicles are owned and used by individual vehicle owners. One way to manage them is to manage RSUs under the national or provincial road authority, while vehicles are managed under regional vehicle registration offices. In addition, as discussed in Sec. 7.6, the inclusion of smartphones as a type of ITS-S in V2P scenarios raises a question of how they are managed to incorporate them as legitimate members of the ITS system. This is another aspect not currently covered by the ETSI ITS standard, thus it requires appropriate specification.

10.4 Absence of Consideration on Post-Quantum Cryptography Technologies

Both ETSI ITS [47] and IEEE 1609.2 [63] use Elliptic Curve Cryptography (ECC) to generate digital signatures and encrypt messages. However, existing public key cryptographic algorithms, including ones based on ECC, are known to be vulnerable in the face of a quantum computer [104]. Because vehicles, as an example of durable goods, have a lifespan as long as 23 years [88], they require technologies that can withstand against cyber threats during their lifetime. This includes migration to quantum-resistant security solutions [53]. When vehicles adopt post-quantum (PQ) digital certificate in the future, a smooth transition from the conventional to new PQ certificates need to be ensured.

Consideration in this area involves two aspects in the V2X context: (1) support of post-quantum cryptography (PQC) technologies, and (2) new issues that stem from the support of such technologies. First, quantum computers are already a reality [85]. Although it is expected to take many years for its capability to become an imminent threat [31], technologies being launched today need to have a solid migration strategy toward PQC paradigm. Evolving capabilities of quantum computers in the future necessitate cycles of updates in affected systems. This may imply that vehicles may require cycles of software update, upgrade, or even hardware replacement during the vehicle's lifetime to stay ahead of threats posed by future evolution of quantum computers. It further introduces a new challenge to securely execute these updates and replacements. This is an uncharted territory involving both vehicles and the underlying system infrastructure. One such example is qSCMS [12] which is a quantum-resistant version of butterfly key [105]. Designing of new solutions to enhance or replace existing mechanisms to support PQ paradigm are required.

Second, support of PQC means that the public key size will increase significantly from the conventional public key schemes. Since 2015, the US National Institute of Standard and Technology (NIST) started the process of selecting PQC [1]. If we assume a code-based quantum-resistant signature algorithm, the size of public key and signature from the ECC-based algorithm increase from 0.1KB to 190KB [67]. This will significantly impact the amount of storage space required in vehicles, especially if a large number of certificates are expected to be preloaded. This will make the preloading of 5 year worth of certificate as proposed in IFAL [110] impractical, if not impossible. This situation will further shift more toward the on-demand based AT reloading strategy we discussed in Sec. 7.3 as a realistic solution.

11 ROOT CAUSE ANALYSIS AND RECOMMENDATIONS

Based on our analysis of ETSI ITS specifications, IEEE WAVE specifications, V2X related EU project documents, and relevant research papers, we have identified and discussed multiple gaps and issues in security aspects of V2X communication. We analyzed each of them and classified their origins into distinct root causes in Table 3. In this table, cells marked with a "✓" indicate a gap in the applicable categories. All of these represent identified

Just Accepted

issues that need further study, research, and solutions. In this section, we clarify each of their root cause category, along with our recommendations for the ETSI ITS specifications to address. Table 4 consolidates the identified issues.

Table 3. SUMMARY OF SECURITY ISSUES

Root Cause Categories	Concerned Section	Conflicting or insufficient specification	Characteristics in vehicle comm. environment	Broadcast based communication	Implementation-dependent ambiguity	Certificate usage and management for vehicles	Certificate management of non-vehicle ITS-S type	RSU infrastructure dependency	MNO involvement and dependency
Sec.6 Privacy protection									
Privacy, Threat Actors, and Vehicle Operation	6.1	✓	✓	✓	✓				
Applicability of Privacy 1: Vehicle Types and Usages	6.2	✓				✓			
Applicability of Privacy 2: Non-Vehicle ITS-S	6.3	✓					✓		
Privacy and Cooperative Awareness	6.4	✓	✓	✓					
Privacy and Road Safety	6.5	✓	✓	✓					
Privacy and Use of Unicast	6.6		✓			✓			
Sec.7: Use of certificate									
Certificate-based Message Verification	7.1	✓	✓		✓				
Certificate Usage and Change Policy	7.2	✓	✓		✓	✓	✓		
Certificate Reloading	7.3	✓			✓	✓		✓	
Certificate Revocation	7.4	✓			✓	✓		✓	✓
Certificate Management of RSUs	7.5	✓			✓		✓	✓	
Certificate Management of VRUs	7.6	✓			✓		✓		✓
Certificate Usage in Multiple Comm.	7.7	✓		✓	✓	✓			
Sec.8: Communication modes									
Broadcast-Oriented Communication	8.1		✓	✓					
Unicast – Confidentiality Protection	8.2		✓						
Sec.9: Message handling									
Plausibility Validation and Misbehavior Detection	9.1	✓	✓		✓				
Communication involving VRU	9.2	✓					✓		✓
Sec.10: System level									
ITS-S Device-dependent Trust Level	10.1	✓		✓				✓	
Interconnection between Multiple Security Management Systems	10.2	✓			✓	✓			
Multiple Security Management Systems for Different ITS-S Types	10.3	✓			✓	✓	✓		✓
Absence of Post-Quantum Cryptography Technologies	10.4	✓							

Just Accepted

Root cause 1: Conflicting or Insufficient Specification. We have identified a number of areas where existing ETSI ITS specifications contain conflicting requirements and areas that are not sufficiently specified. Conflicting requirements likely lead to an ineffective system as the end result. Insufficient specification means certain security aspects are specified for a certain subset only, or implicitly left to implementation decisions.

Recommendations & research objectives:

- Solve the conflicting requirements between privacy, anonymity, and safety – this refers to the situation where the mechanisms to ensure privacy of a vehicle owner result in potential compromise in road safety. One example is the unobservability property making vehicles not being able to determine whether to apply brake or not upon receiving EEBL message from a surrounding vehicle (Sec. 6.5). Another example is the certificate management of non-vehicle ITS-S types (Sec. 6.3, 7.5, 7.6, and 9.2).
- Clarify the relationship and define the interworking mechanism between security management systems of different organizational entities, jurisdictions, and countries – vehicles from multiple regions and countries need to be able to communicate seamlessly across boundaries. This includes validation of pseudonym certificates in the receives messages, plausibility validation, and misbehavior detection (Sec. 9.1 and 10.2).
- The integration and joint risk assessment of complex system requirements that encompass safety, security, and privacy is a poorly understood field of research. Analysis techniques that combine approaches from safety engineering with those from security engineering, e.g. STPA-Sec or integrating attack vectors with fault trees may help but have not been applied to systems at the scale of V2X.

Root cause 2: Characteristics of Vehicular Communication Environment. The fundamental characteristic of a vehicle in operation is its dynamically changing position, both in relation to a static geo-referential or other vehicles in operation. The paradigm of constant topological changes combined with short-range direct communication poses challenges. This also applies to GeoNetworking as it is a chain of short-range communication between vehicles. This fundamental characteristic likely limits the type of services that can be realized in such environment. In particular, direct communications that are expected to last longer or between specific endpoints in unicast mode may suffer from a communication loss and impact its services as a result.
Recommendations & research objectives:

- Establish realistic expectations of the communication in both broadcast and unicast modes. Articulate the criteria and condition to use unicast communication as vehicles at the borderline of communication range will likely suffer communication failure (Sec. 6.6, 8.2).
- Establish guidelines on how to use and change pseudonyms for different purposes effectively in dynamically changing topology (Sec. 7.2, 7.7).
- A potential avenue towards increasing fault tolerance of V2X networks is to improve peer-to-peer networking between road users. To improve road safety, V2X technology must be used together with direct sensor perceptions in autonomous vehicles.

Root cause 3: Broadcast Based Communication. Basic services in the V2X are CAM and DENM which are broadcast based communication. Its fundamental characteristics are that: 1) any entity can receive messages, and 2) confidentiality protection is not applied. These two points render CAM and DENM *open* communication. There are solutions to apply encryption to broadcast traffic [30, 57, 59, 99]. However, the ETSI ITS standard does not require such mechanism. This situation makes it trivial for a malicious entity to eavesdrop and collect data (cf. Sec. 8.1). The only solution to render vehicular communication trustworthy is to apply the PKI-based message authentication and validation mechanism [7]. This makes V2X infrastructure dependent on security and reliability of PKI systems.
Recommendations & research objectives:

- Consider alternative approaches to apply confidentiality protection or pseudonymity to the broadcast-based communication, investigate efficient means for cryptographic credential and trust management at scale.

Root cause 4: Implementation-Dependent Ambiguity. We discussed the challenges, such as CRL distribution, plausibility validation, and misbehaviour detection. These areas are often implementation specific and are left up to the individual OEM's decision. This situation results in variations of effectiveness among implementations,

Just Accepted

where one implementation performs better than others in real life. It is likely not realistic to specify every aspects of the communication system in the standard. In fact, it may make sense or is inevitable to leave some aspects to implementation choice. However, those aspects should at least be documented in the standard to be cognizant of the choice of the extent the standard does not cover. This way, possible consequences are made clear.
Recommendations & research objectives:

- Define baseline criteria, which consists of a set of test cases, test data, and resulting decision criteria as a common foundation upon which various implementations can be tested and evaluated against. Doing so has a number of benefits (Sec. 9.1.1). One example is to define a clear and unambiguous method to validate plausibility and detect misbehaviour (Sec. 9.1).

Root cause 5: Certificate Usage and Management for Vehicles. Vehicles' usage of pseudonym certificates is not well defined in ETSI ITS specifications. This includes their usage period, change rules, and reloading mechanisms. In addition, another unspecified area is the pseudonym usage for different purposes (e.g. broadcast and unicast).
Recommendations & research objectives:

- Define how pseudonym and certificate are used by vehicles. This includes usage and change rules (Sec. 7.2), revocation and reloading rules and policy (Sec. 7.3, 7.7).
- Investigate efficient means for cryptographic credential and trust management at scale, consider the use of light-weight Hardware Security Modules (HSM) and Trusted Execution Environments (TEE) in vehicles.

Root cause 6: Certificate Management of Non-Vehicle ITS-S Types. Pseudonym usage by RSUs is not explicitly specified in the ETSI ITS standard. Thus it remains unclear if and how their usage is different from vehicles. Introducing smartphones (VRU) as a type of ITS-S requires appropriate management of these devices. Smartphones are consumer-owned generic platform as opposed to dedicated purpose devices such as OBUs and RSUs, thus a different approach to manage them will be required. Another open issue of smartphones is whether and how they can be revoked and removed from ITS system, if and when it is necessary.
Recommendations & research objectives:

- Define how the pseudonym usage in RSU is different from vehicles (Sec. 7.5). Define how smartphones as a type of ITS-S is managed in the ITS system, including enrolment, verification, and authorization, issuance of certificates, usage of pseudonyms, and how they are revoked from the system (Sec. 7.6).

Root cause 7: RSU Infrastructure Dependency. Many functionalities discussed in EU project use cases depend on RSUs and the infrastructure behind them, such as distribution and reloading of certificates. However, ubiquitous installation and availability of RSUs is an assumption, not a given condition. How soon an RSU infrastructure will be deployed depends on a number of non-technical factors, such as government policy on ITS and budget allocation. It is likely a gradual process and varies from one region to another and one country to another. ITS-capable vehicles likely find themselves in the situation where RSU installation is either scarce or non-existent. Thus, being overly dependent on RSUs is counterproductive to the deployment of V2X technology.
Recommendations & research objectives:

- Define alternative solutions to reduce dependency on the ubiquitous RSU deployment in such a way that necessary functionalities can be fulfilled independent from RSUs when it is necessary, while making effective use of RSUs when they are available (Sec. 7.3).

Root cause 8: MNO Involvement and Dependency. Within the context of VRUs, whether interaction is required between the ITS system and MNOs to manage their access to the ITS system is unspecified in the ETSI ITS specification. If required, the solution needs standardization so that it will be adopted by all MNOs at international level.
Recommendations & research objectives:

Just Accepted

- Define if the ITS management system and MNOs need to interact with each other to manage VRUs (smartphones) or not. This interaction between them includes definition of message contents (Sec. 7.6). This involves coordination with appropriate standard bodies such as 3GPP.

Table 4. LIST OF RECOMMENDED ACTIONS TO ETSI ITS SPECIFICATIONS

Num	Description	Section
1	Specify possible differences in the privacy protection requirements for different ITS-S types.	6.2, 6.3
2	Resolve conflicting requirements of privacy protection and including vehcile-identifiable information in CAM and DENM.	6.4
3	Resolve conflicting requirements of privacy protection and road safety.	6.1, 6.5
4	Resolve privacy protection in unicast communication from both internal and external threats.	6.6
5	Address the potential issue of real-time certificate validation.	7.1
6	Standardise certificate change and reloading rule or policy.	7.2, 7.3
7	Resolve the time gap associated with passive revocation.	7.4
8	Specify certificate management of RSUs and VRUs.	7.5, 7.6
9	Specify different use of certificates for different purposes.	7.7
10	Address vulnerabilities of broadcast messages against passive observers.	8.1
11	Establish guidances on the use of unicast mode.	8.2
12	Establish guidance on the implementation of plausibility validation and misbehaviour detection.	9.1
13	Investigate solutions for accurate detection of VRU movement to VAM.	9.2
14	Consider possible notion of device type-dependent trust level.	10.1
15	Analyse and establish scenarios of interconnecting multiple management systems.	10.2, 10.3

12 CONCLUSION AND FUTURE WORK

In this paper, we examined the EU standards for ITS, related US standards, various V2X-related EU projects, and relevant research papers. We integrated information from these sources, analyzed, and identified gaps in the security aspects of vehicular communication, focusing on the ETSI ITS specifications.

The issues and gaps we have identified are significant. They include conflicting and undefined specification in the standards. System level aspects need further definition, e.g. interworking of multiple management systems across multiple jurisdictions and countries. The security management of VRUs (smartphones) as a new ITS-S type is missing. Without addressing these aspects, the vehicular communication in reality can very well be unreliable, insecure, and unusable, ultimately leading to accidents, injuries, or loss of properties. Leaving details to implementation-specific solutions can lead to varying degree of effectiveness among implementations. To ensure uniform operation and effectiveness, further research and standardization is needed. In this respect, the future work is to address these gaps and issues to define possible solutions.

As a conclusion, the security solution in the ITS standards solely based on PKI leaves a number of areas to reconsider. Additional approaches and solutions are required to ensure vehicular communication is indeed secure so that the overall objective to make roads safer and reduce road accidents can be achieved rather than providing a new target for cyberattacks. The fundamental nature of cyber-physical system, such as vehicular communication, is that a sub-optimal system can cause physical damage in reality. In order to avoid such losses, all relevant security and privacy aspects of vehicular communication need to be addressed.

Just Accepted

ACKNOWLEDGMENTS

This work was supported in part by CyberSecurity Research Flanders with reference number VR20192203. This work was also supported in part by the Research Council KU Leuven C1 on Security and Privacy for Cyber-Physical Systems and the Internet of Things with contract number C16/15/058. In addition, this work was supported in part by the Flemish Government through the imec Netsec project, through the EIT Health RAMSES

project, through the Smart Highways SErVo project, and by the European Commission through the Horizon 2020 research and innovation programme under grant agreement H2020-SC1-FA-DTS-2018-1-826284 ProTego and MSCA-ITN-814035 5GhOSTS.

REFERENCES

[1] [n.d.]. Post-Quantum Cryptography Standardization. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization. Accessed: 2021-12-03.
[2] 3GPP. 2019. *Architecture enhancements for V2X services.* Technical Specification (TS) 23.285. 3rd Generation Partnership Project (3GPP). Version 16.2.0.
[3] 3GPP. 2020. *Study on Security Aspects of 3GPP support for Advanced V2X Services.* Technical Report (TR) 33.836. 3rd Generation Partnership Project (3GPP). Version 16.0.0.
[4] 3GPP. 2021. *Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services.* Technical Specification (TS) 23.287. 3rd Generation Partnership Project (3GPP). Version 17.2.0.
[5] 5G-Mobix. [n.d.]. *5G for cooperative & connected automated MOBIility on X-border corridors.* Retrieved Aug 26, 2021 from https://www.5g-mobix.com
[6] NIS Act. 2019. Cybersecurity Act. *OJ L* 194, 19.7 (2019).
[7] Carlisle Adams and Steve Lloyd. 2003. *Understanding PKI: concepts, standards, and deployment considerations.* Addison-Wesley Professional.
[8] Aljawharah Alnasser, Hongjian Sun, and Jing Jiang. 2019. Cyber security challenges and solutions for V2X communications: A survey. *Computer Networks* 151 (2019), 52–67.
[9] Moreno Ambrosin, Lily L Yang, Xiruo Liu, Manoj R Sastry, and Ignacio J Alvarez. 2019. Design of a Misbehavior Detection System for Objects Based Shared Perception V2X Applications. In *2019 IEEE Intelligent Transportation Systems Conference (ITSC)*. IEEE, 1165–1172.
[10] Nick Asselin-Miller, Marius Biedka, Gena Gibson, Felix Kirsch, Nikolas Hill, Ben White, and Kotub Uddin. 2016. Study on the deployment of C-ITS in Europe: Final Report. *Report for DG MOVE MOVE/C* 3 (2016), 2014–794.
[11] Radu Alexandru Badea and Lucian Stanciu. 2018. A Survey and Research Model for Vehicular Communication and Security Challenges. In *2018 International Conference on Communications (COMM)*. IEEE, 291–296.
[12] Paulo SLM Barreto, Jefferson E Ricardini, Marcos A Simplicio Jr, and Harsh Kupwade Patil. 2018. qSCMS: Post-quantum certificate provisioning process for V2X. *IACR Cryptol. ePrint Arch.* 2018 (2018), 1247.
[13] Giampaolo Bella, Pietro Biondi, Gianpiero Costantino, and Ilaria Matteucci. 2019. Toucan: A protocol to secure controller area network. In *Proceedings of the ACM Workshop on Automotive Cybersecurity*. 3–8.
[14] Norbert Bißmeyer. 2014. Misbehavior detection and attacker identification in vehicular ad-hoc networks, PhD thesis. (2014).
[15] Norbert Bißmeyer, Hagen Stübing, Elmar Schoch, Stefan Götz, Jan Peter Stotz, and Brigitte Lonc. 2011. A generic public key infrastructure for securing car-to-x communication. In *18th ITS World Congress on Intelligent Transport Systems*, Vol. 14.
[16] Benedikt Brecht. 2016. Security and Privacy for a Connected Vehicle Environment. (2016).
[17] Benedikt Brecht, Dean Therriault, André Weimerskirch, William Whyte, Virendra Kumar, Thorsten Hehn, and Roy Goudy. 2018. A security credential management system for V2X communications. In *2018 IEEE Transactions on Intelligent Transportation Systems*. IEEE, 3850–3871.
[18] Jin Cao, Maode Ma, Hui Li, Ruhui Ma, Yunqing Sun, Pu Yu, and Lihui Xiong. 2019. A Survey on Security Aspects for 3GPP 5G Networks. *IEEE Communications Surveys & Tutorials* 22, 1 (2019), 170–195.
[19] 5G Car. [n.d.]. *Fifth Generation Communication Automotive Research and innovation.* Retrieved Aug 26, 2021 from http://5gcar.eu
[20] 5G Carmen. [n.d.]. *5G for Connected and Automated Road Mobility in the European UnioN.* Retrieved Aug 26, 2021 from https://5gcarmen.eu/
[21] Alishah Chator and Matthew Green. 2018. Don't Talk to Strangers-On the Challenges of Intelligent Vehicle Authentication.. In *VEHITS*. 522–528.
[22] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage. 2011. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *USENIX Sec*.
[23] European Commission. 2017. Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS). *C-ITS Platform Phase II* (2017).
[24] European Commission. 2018. Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Rel.1.1. *C-ITS Platform Phase II* (2018).
[25] Concorda. [n.d.]. *Connected Corridor for Driving Automation.* Retrieved Aug 26, 2021 from https://connectedautomateddriving.eu/project/concorda
[26] Quentin Covert, Dustin Steinhagen, Mary Francis, and Kevin Streff. 2020. Towards a triad for data privacy. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*.

Just Accepted

[27] 5G CroCo. [n.d.]. *Fifth Generation Cross-Border Control.* Retrieved Aug 26, 2021 from https://5gcroco.eu/
[28] Vijay Devarapalli, Ryuji Wakikawa, Alexandru Petrescu, and Pascal Thubert. [n.d.]. IETF RFC 3963-Network Mobility (NEMO) Basic Support Protocol. Online document. Updated in January 2005. Cited on 2.2. 2011.
[29] NIS Directive. 2016. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *OJ L* 194, 19.7 (2016), 2016.
[30] Xinjun Du, Ying Wang, Jianhua Ge, and Yumin Wang. 2005. An ID-based broadcast encryption scheme for key distribution. *IEEE Transactions on broadcasting* 51, 2 (2005), 264–266.
[31] Ericsson. 2021. Ensuring Security in Mobile Nnetworks Post-Quantum. *Ericsson Technology Review* 12 (2021).
[32] Stephan Escher, Markus Sontowski, Knut Berling, Stefan Köpsell, and Thorsten Strufe. 2021. How well can your car be tracked: Analysis of the European C-ITS pseudonym scheme. In *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*. IEEE, 1–6.
[33] ETSI. 2010. *Intelligent Transport Systems (ITS); Communications Architecture.* European Standard (EN) EN 302 665. European Telecommunications Standard Institute (ETSI). Version 1.1.1.
[34] ETSI. 2010. *Intelligent Transport Systems (ITS); Security; Security Services and Architecture.* Technical Specification (TS) TS 102 731. European Telecommunications Standard Institute (ETSI). Version 1.1.1.
[35] ETSI. 2010. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements.* Technical Specification (TS) TS 102 637-1. European Telecommunications Standard Institute (ETSI). Version 1.1.1.
[36] ETSI. 2012. *Intelligent Transport Systems (ITS); Security; Access Control Technical Specification.* Technical Specification (TS) TS 102 942. European Telecommunications Standard Institute (ETSI). Version 1.1.1.
[37] ETSI. 2012. *Intelligent Transport Systems (ITS); Security; Confidentiality services.* Technical Specification (TS) TS 102 943. European Telecommunications Standard Institute (ETSI). Version 1.1.1.
[38] ETSI. 2014. *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements.* European Standard (EN) EN 302 636-1. European Telecommunications Standard Institute (ETSI). Version 1.2.1.
[39] ETSI. 2014. *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network Architecture.* European Standard (EN) EN 302 636-3. European Telecommunications Standard Institute (ETSI). Version 1.2.1.
[40] ETSI. 2014. *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols.* European Standard (EN) EN 302 636-6-1. European Telecommunications Standard Institute (ETSI). Version 1.2.1.
[41] ETSI. 2017. *Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA).* Technical Report (TR) TR 102 893. European Telecommunications Standard Institute (ETSI). Version 1.2.1.
[42] ETSI. 2017. *Intelligent Transport Systems (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality.* European Standard (EN) EN 302 636-4-1. European Telecommunications Standard Institute (ETSI). Version 1.3.1.
[43] ETSI. 2018. *Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management.* Technical Report (TR) TR 103 415. European Telecommunications Standard Institute (ETSI). Version 1.1.1.
[44] ETSI. 2019. *Intelligent Transport Systems (ITS) Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service.* European Standard (EN) EN 302 637-2. European Telecommunications Standard Institute (ETSI). Version 1.4.1.
[45] ETSI. 2019. *Intelligent Transport Systems (ITS). Vehicular Communications; Basic Set of Applications; Part 3: Specification of Decentralized Environmental Notification Basic Service.* European Standard (EN) EN 302 637-3. European Telecommunications Standard Institute (ETSI). Version 1.3.1.
[46] ETSI. 2021. *Intelligent Transport Systems (ITS); Security, ITS communications security architecture and security management.* Technical Specification (TS) TS 102 940. European Telecommunications Standard Institute (ETSI). Version 2.1.1.
[47] ETSI. 2021. *Intelligent Transport Systems (ITS); Security; Security header and certificate formats.* Technical Specification (TS) TS 103 097. European Telecommunications Standard Institute (ETSI). Version 2.1.1.
[48] ETSI. 2021. *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management.* Technical Specification (TS) TS 102 941. European Telecommunications Standard Institute (ETSI). Version 2.1.1.
[49] ETSI. 2021. *Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) awareness; Part 1: Use Cases definition; Release 2.* Technical Report (TR) TR 103 300-1. European Telecommunications Standard Institute (ETSI). Version 2.2.1.
[50] ETSI. 2021. *Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) awareness; Part 2: Functional Architecture and Requirements definition; Release 2.* Technical Specification (TS) TS 103 300-2. European Telecommunications Standard Institute (ETSI). Version 2.2.1.
[51] ETSI. 2021. *Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) awareness; Part 3: Specification of VRU awareness basic service; Release 2.* Technical Specification (TS) TS 103 300-3. European Telecommunications Standard Institute (ETSI). Version 2.1.2.
[52] Antonio E Fernandez, Mikael Fallgren, and Nadia Brahmi. 2019. 5GCAR scenarios, use cases, requirements and KPIs. *Fifth Generation Communication Automotive Research and innovation, Tech. Rep. D* 2 (2019).
[53] Tiago M Fernández-Caramés. 2019. From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. *IEEE Internet of Things Journal* 7, 7 (2019), 6457–6480.

Just Accepted

[54] Flightradar24.com. [n.d.]. . Retrieved June 1, 2022 from https://www.flightradar24.com
[55] Laurent Gallo and Massimo Condoluci. 2019. 5GCAR D4.2 Final Design and Evaluation of the 5G V2X System Level Architecture and Security Framework. *Fifth Generation Communication Automotive Research and innovation, Tech. Rep. D* (2019).
[56] Laurent Gallo, Thierry Lejkin, Bruno Tossou, and Bernadette Villeforceix. 2018. Initial Design of 5G V2X System Level Architecture and Security Framework. *Fifth Generation Communication Automotive Research and innovation, Tech. Rep. D* 2 (2018).
[57] Juan A Garay, Jessica Staddon, and Avishai Wool. 2000. Long-lived broadcast encryption. In *Annual International Cryptology Conference*. Springer, 333–352.
[58] Amrita Ghosal and Mauro Conti. 2020. Security issues and challenges in V2X: A survey. *Computer Networks* 169 (2020), 107093.
[59] Dani Halevy and Adi Shamir. 2002. The LSD broadcast encryption scheme. In *Annual International Cryptology Conference*. Springer, 47–60.
[60] Monowar Hasan, Sibin Mohan, Takayuki Shimizu, and Hongsheng Lu. 2020. Securing Vehicle-to-Everything (V2X) Communication Platforms. *IEEE Transactions on Intelligent Vehicles* (2020).
[61] Jiaqi Huang, Dongfeng Fang, Yi Qian, and Rose Qingyang Hu. 2020. Recent advances and challenges in security and privacy for v2x communications. *IEEE Open Journal of Vehicular Technology* 1 (2020), 244–266.
[62] IEEE. 2016. *IEEE Standard for Information technology-Telecommunication and information exchange between systems-Local and metropolitan area networks-Specific requirements Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment1: Radio Resource Measurement of Wireless LANs.* Standard. IEEE 802 LAN/MAN Standards Committee.
[63] IEEE. 2016. *IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages.* Standard Std 1609–2. Institute of Electrical and Electronics Engineers (IEEE).
[64] ISO. 2018. *Road vehicles — Functional safety.* Standard ISO 26262. International Organization for Standardization (ISO).
[65] ISO. 2021. *Road vehicles — Cybersecurity engineering.* Standard ISO/SAE 21434. International Organization for Standardization (ISO).
[66] iso39001. 2012. *Road traffic safety (RTS) management systems — Requirements with guidance for use.* Standard ISO 39001. International Organization for Standardization (ISO).
[67] Panos Kampanakis, Peter Panburana, Ellie Daw, and Daniel Van Geest. 2018. The Viability of Post-quantum X. 509 Certificates. *IACR Cryptol. ePrint Arch.* 2018 (2018), 63.
[68] Mohammad Khodaei and Panagiotis Papadimitratos. 2020. Scalable & resilient vehicle-centric certificate revocation list distribution in vehicular communication systems. *IEEE Transactions on Mobile Computing* (2020).
[69] Florian Klingler, Falko Dressler, and Christoph Sommer. 2015. IEEE 802.11p unicast considered harmful. In *2015 IEEE Vehicular Networking Conference (VNC)*. IEEE, 76–83.
[70] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, et al. 2010. Experimental security analysis of a modern automobile. In *2010 IEEE Symposium on Security and Privacy*. IEEE, 447–462.
[71] Kenneth P Laberteaux, Jason J Haas, and Yih-Chun Hu. 2008. Security certificate revocation list distribution for VANET. In *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*. 88–89.
[72] Chengzhe Lai, Rongxing Lu, Dong Zheng, and Xuemin Sherman Shen. 2020. Security and privacy challenges in 5G-enabled vehicular networks. *IEEE Network* 34, 2 (2020), 37–45.
[73] Stéphanie Lefevre, Jonathan Petit, Ruzena Bajcsy, Christian Laugier, and Frank Kargl. 2013. Impact of v2x privacy strategies on intersection collision avoidance systems. In *2013 IEEE Vehicular Networking Conference*. IEEE, 71–78.
[74] Rongxing Lu, Lan Zhang, Jianbing Ni, and Yuguang Fang. 2019. 5G vehicle-to-everything services: Gearing up for security and privacy. *Proc. IEEE* 108, 2 (2019), 373–389.
[75] Xiaomin Ma, Xianbo Chen, and Hazem H Refai. 2009. Performance and reliability of DSRC vehicular safety communication: a formal analysis. *EURASIP Journal on Wireless Communications and Networking* 2009 (2009), 1–13.
[76] Georg Macher, Christoph Schmittner, Omar Veledar, and Eugen Brenner. 2020. ISO/SAE DIS 21434 automotive cybersecurity standard-in a nutshell. In *International Conference on Computer Safety, Reliability, and Security*. Springer, 123–135.
[77] MarineTraffic.com. [n.d.]. . Retrieved June 1, 2022 from https://www.marinetraffic.com
[78] Vuk Marojevic. 2018. C-V2X security requirements and procedures: Survey and research directions. *arXiv preprint arXiv:1807.09338* (2018).
[79] Ángel Martin and Gorka Vélez. 2019. 5G-enabled CCAM use cases specifications. *5G Mobix* 2 (2019).
[80] McKinsey. [n.d.]. *Cybersecurity in automotive, mastering the challenge.* Retrieved June 30, 2022 from https://www.mckinsey.com/industries/automotive-and-assembly/our-insights
[81] Charlie Miller and Chris Valasek. 2015. Remote exploitation of an unaltered passenger vehicle. *Black Hat USA* (2015).
[82] Mujahid Muhammad and Ghazanfar Ali Safdar. 2018. Survey on existing authentication issues for cellular-assisted V2X communication. *Vehicular Communications* 12 (2018), 50–65.
[83] Hyeran Mun, Kyusuk Han, and Dong Hoon Lee. 2020. Ensuring safety and security in CAN-based automotive embedded systems: A combination of design optimization and secure communication. *IEEE Transactions on Vehicular Technology* 69, 7 (2020), 7078–7091.

Just Accepted

[84] Dries Naudts, Vasilis Maglogiannis, and Simon Vanneste. 2018. Test site BE operational- Belgian Pilot site. *Concorda* 2 (2018).
[85] NewScientist.com. [n.d.]. *IBM unveils its first commercial quantum computer.* Retrieved Nov 09, 2021 from https://www.newscientist.com/article/2189909-ibm-unveils-its-first-commercial-quantum-computer/
[86] NHTSA. 2016. Preliminary Regulatory Impact Analysis, FMVSS No. 150 Vehicle-To-Vehicle Communication Technology for Light Vehicles. *NHTSA* 2 (2016).
[87] Michael E Nowatkowski and Henry L Owen. 2010. Certificate revocation list distribution in VANETs using Most Pieces Broadcast. In *Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon)*. IEEE, 238–241.
[88] Masahiro Oguchi and Masaaki Fuse. 2015. Regional and longitudinal estimation of product lifespan distribution: a case study for automobiles and a simplified estimation method. *Environmental science & technology* 49, 3 (2015), 1738–1743.
[89] Aleksandr Ometov and Sergey Bezzateev. 2017. Multi-factor authentication: A survey and challenges in V2X applications. In *2017 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. IEEE, 129–136.
[90] Panagiotis Papadimitratos, Ghita Mezzour, and Jean-Pierre Hubaux. 2008. Certificate revocation list distribution in vehicular communication systems. In *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*. 86–87.
[91] European Parliament. 2002. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Off. *JL 201, 31.7. 2002, at 37.(Directive on Privacy and Electronic Communications)* (2002).
[92] Eric Perraud and Kurt Eckert. 2019. Test Case Definition and Test Site Description Part 1. *5G CroCo* 2 (2019).
[93] Andreas Pfitzmann and Marit Hansen. 2010. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. (2010).
[94] Han Qiu, Meikang Qiu, and Ruqian Lu. 2019. Secure V2X Communication Network based on Intelligent PKI and Edge Computing. *IEEE Network* (2019).
[95] Protection Regulation. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council. *REGULATION (EU)* 679 (2016), 2016.
[96] Giovanni Rigazzi, Andrea Tassi, Robert J Piechocki, Theo Tryfonas, and Andrew Nix. 2017. Optimized certificate revocation list distribution for secure V2X communications. In *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*. IEEE, 1–7.
[97] Ishtiaq Rouf, Robert D Miller, Hossen A Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser, Wade Trappe, and Ivan Seskar. 2010. Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study.. In *USENIX Security Symposium*, Vol. 10.
[98] SAE. 2009. *J2735: Dedicated Short Range Communications (DSRC) message set dictionary.* Standard SAE J2735:2009. SAE International.
[99] Ryuichi Sakai and Jun Furukawa. 2007. Identity-Based Broadcast Encryption. *IACR Cryptol. ePrint Arch.* 2007 (2007), 217.
[100] Alexey Samoshkin. [n.d.]. *SSL certificate revocation and how it is broken in practice.* Retrieved Sept 16, 2021 from https://medium.com/@alexeysamoshkin/how-ssl-certificate-revocation-is-broken-in-practice-af3b63b9cb3
[101] Stefan Santesson, Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams. 2013. X. 509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP. *RFC* 6960 (2013), 1–41.
[102] Christoph Schmittner, Gerhard Griessnig, and Zhendong Ma. 2018. Status of the Development of ISO/SAE 21434. In *European Conference on Software Process Improvement*. Springer, 504–513.
[103] SCOOP. [n.d.]. *SCOOP.* Retrieved Aug 26, 2021 from http://www.scoop.developpement-durable.gouv.fr/en/
[104] Peter W Shor. 1999. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review* 41, 2 (1999), 303–332.
[105] Marcos A Simplicio, Eduardo Lopes Cominetti, Harsh Kupwade Patil, Jefferson E Ricardini, and Marcos Vinicius M Silva. 2018. The unified butterfly effect: Efficient security credential management system for vehicular communications. In *2018 IEEE Vehicular Networking Conference (VNC)*. IEEE, 1–8.
[106] Adam Slagell, Rafael Bonilla, and William Yurcik. 2006. A survey of PKI components and scalability issues. In *2006 IEEE International Performance Computing and Communications Conference*. IEEE, 10–pp.
[107] Syrma SGS Technology. [n.d.]. *Automotive ECU: Core Component for Connected Cars.* Retrieved May 31, 2022 from https://www.syrma.com/ecu/
[108] IoT World Today. 2022. Connectivity Changes How Customers, Manufacturers Look at Vehicles. https://iotworldtoday.tradepub.com/free/w_defa2552/prgm.cgi. (2022). Accessed: May 27, 2022.
[109] Rens Wouter van der Heijden, Stefan Dietzel, Tim Leinmüller, and Frank Kargl. 2018. Survey on misbehavior detection in cooperative intelligent transportation systems. *IEEE Communications Surveys & Tutorials* 21, 1 (2018), 779–811.
[110] Eric Verheul, Christopher Hicks, and Flavio D Garcia. 2019. Ifal: Issue first activate later certificates for v2x. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 279–293.
[111] Filippo Visintainer (Ed.). 2019. 5G CARMEN Use Cases and Requirements. *5G CARMEN* 2 (2019).
[112] Skanda Vivek, David Yanni, Peter J Yunker, and Jesse L Silverberg. 2019. Cyberphysical risks of hacked internet-connected vehicles. *Physical Review E* 100, 1 (2019), 012316.

Just Accepted

[113] Qianpeng Wang, Deyun Gao, and Du Chen. 2020. Certificate Revocation Schemes in Vehicular Networks: A Survey. *IEEE Access* 8 (2020), 26223–26234.

[114] Takahito Yoshizawa and Bart Preneel. 2019. Survey of Security Aspect of V2X Standards and Related Issues. In *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 1–5.

Just Accepted