# Cyber Security Standards and Issues in V2X Communications for Internet of Vehicles

*I Ivanov*, C Maple*, T Watson*, S Lee* [†]

* WMG, Warwick University, UK, ii@warwick.ac.uk, cm@warwick.ac.uk, tw@warwick.ac.uk,
[†] Electronics and Telecommunication Research Institute, South Korea, ttomlee@etri.re.kr

**Keywords:** V2X, ITS, DSRC, cyber security, connected vehicles.

## Abstract

Significant developments have taken place over the past few years in the area of vehicular communication systems in the ITS environment. It is vital that, in these environments, security is considered in design and implementation since compromised vulnerabilities in one vehicle can be propagated to other vehicles, especially given that V2X communication is through an ad-hoc type network. Recently, many standardisation organisations have been working on creating international standards related to vehicular communication security and the so-called Internet of Vehicles (IoV). This paper presents a discussion of current V2X communications cyber security issues and standardisation approaches being considered by standardisation bodies such as the ISO, the ITU, the IEEE, and the ETSI.

## 1 Introduction

The area of Vehicle-to-Everything (V2X) communications has become an increasingly popular research topic within mobile wireless networking, and is attracting significant attention from governmental, research and industry organisations. Connected vehicle technologies aim to tackle some of the biggest challenges in Intelligent Transport Systems (ITS) in the areas of safety, mobility, and environment. Since ITS efficiency directly depends on V2X communications, a variety of cyber-threats and attacks can affect impact on functionality and integrity.

ITS use technologies that allow road vehicles to communicate with other vehicles, with pedestrians and roadside infrastructure. These systems are also known as Vehicle-to-Everything (V2X) communications and contain three different types as shown: Vehicle-to-Infrastructure (V2I) communications; Vehicle-to-Vehicle (V2V) communications; and Vehicle-to-Pedestrian (V2P) communications.

A typical vehicular communication system used in ITS is responsible for exchanging data between vehicles (V2V) and between a vehicle and infrastructure (V2I). This can include information and warnings derived from the on-board sensors, such as current position and speed of the vehicle. In addition, roadside units (RSU) are able to communicate with traffic monitoring systems that collect and distribute warnings about hazardous situations. ITS implemented without appropriate security measures can have serious consequences when compromised, jeopardising traffic safety and lives of the drivers. The security of ITS should therefore be investigated in order to enable the successful deployment of V2X communications in an ITS environment.

## 2 Related work

Cyber security in V2X communications for ITS has been addressed by various researchers recently. Several surveys exist that discuss the research challenges regarding the dynamic adaptation of the security features and interplay between safety and security in ITS.

The authors of [1] have reviewed the current research challenges and opportunities related to the development of secure and safe ITS applications. They first explore the architecture and main characteristics of ITS systems and survey the key enabling standards and projects. Then, various ITS security threats are analysed and classified, along with corresponding cryptographic countermeasures. In order to better investigate the issues arising from high complexity and communication overhead of the security algorithms, the authors presented a detailed ITS safety application case study in light of the European ETSI TC ITS standard. In [2] the author presents different types of communication technologies used in the modern IoT world, discussing issues and challenges, illustrated through a number of key applications.

Various authors have identified different security vulnerabilities and threats and propose a range of security measures for ITS communications. The authors of [3] have presented a methodical approach to balance the security costs for implementing vehicular security measures against the security risks of corresponding automotive security attacks. The work is based upon well-established methodologies, which have been carefully adapted for ITS scenarios. The approach is based on the assumption that the probability of a successful attack on a security measure decreases with the increase of the attack potential required. However, they stress that this is only true for most, but not all, real-world scenarios and even if based on well-found analyses – a risk assessment remains a statistical estimation that inherently includes uncertainties.

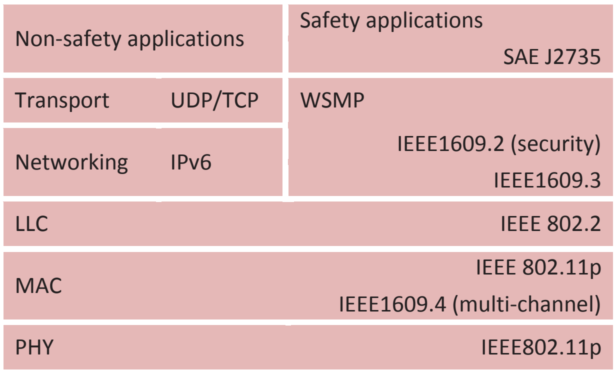
## 3 Wireless Access Technologies for V2X

Various communications technologies are available to provide the radio environment required by the vehicular networks in ITS, such as Dedicated Short-Range Communications (DSRC or IEEE 802.11p), Long Term Evolution (LTE), Worldwide Interoperability for Microwave Access (WiMAX/IEEE802.16), Infrared communications, Bluetooth, ZigBee (IEEE 803.15.4), and so forth. We describe some of the key technologies

### 3.1 Dedicated Short-Range Communications (DSRC)

Traditional IEEE 802.11 Media Access Control (MAC) operations suffer from significant overheads when used in V2X scenarios. To address the challenging V2X requirements, the DSRC initiative was launched. The Institute of Electrical and Electronics Engineers (IEEE) adopted the DSRC proposals and developed an amendment to the IEEE 802.11, provided in 802.11p. This new amendment, specifies maximum delays of tens of milliseconds for high-priority messages. Technically, a spectrum band is allocated in 5.9 GHz for priority road safety applications, for V2V and V2I communications.

Work on the standardisation of additional layers includes the IEEE 1609.x family of standards that specify multichannel operation, networking services, resource manager and security services. The combination of IEEE 802.11p and the IEEE 1609 protocol suite comprise to give Wireless Access in Vehicular Environments (WAVE). Collectively the IEEE 1609.x family, IEEE 802.11p and the SAE J2735 form the key parts of the currently proposed WAVE protocol stack. The WAVE protocol architecture [4], with its major components, is shown in Figure 1.



| | | |
|---|---|---|
| Non-safety applications | | Safety applications<br>SAE J2735 |
| Transport | UDP/TCP | WSMP<br>IEEE1609.2 (security)<br>IEEE1609.3 |
| Networking | IPv6 | |
| LLC | | IEEE 802.2 |
| MAC | | IEEE 802.11p<br>IEEE1609.4 (multi-channel) |
| PHY | | IEEE802.11p |

Figure 1: The WAVE protocol stack and its associated standards

Although DSRC was the first standard specifically created for road communications, it has already identified disadvantages such as limited frequency spectrum available for V2V safety (10MHz for the United States and 30MHz for Europe); low reliability [5]; unbounded delay and intermittent V2I connectivity [6].

The physical layer of DSRC is compliant with the profile of IEEE 802.11 - orthogonal frequency division multiplexing (OFDM) PHY specification for the 5 GHz band [7], as specified in details for ITS in [8] and shown in Figure 2, where HPPS is High Power Public Safety; Ctrl is Control Channel; CSL is Critical safety of live or Collision Avoidance Safety channel; and GB is Guard band.

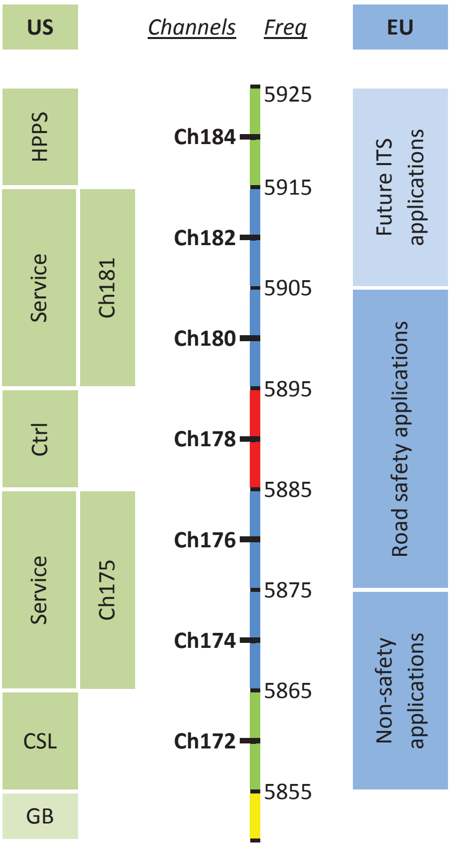


Figure 2: DSRC frequency allocation in Europe and US

There are three types of intentional interferences in V2X communications which can be considered as cyber security threats at the physical layer: jamming, spoofing, and meaconing. For jamming, a signal (DSRC, LTE-V, GPS, etc.) is continuously transmitted with enough power to prevent the receiver from acquiring the information within the area of communication. For spoofing, a deceptive signal is transmitted on the same frequency of V2X as the legitimate signal. Spoofing is intended to deceive the V2X receiver without being recognised, since the receiver treats the spoofing signal as real, though it is a counterfeit signal. For meaconing, this involves the retransmission of the V2X signal after a delaying, and broadcasting the signal in the same frequency as the real signal thereby confusing the ITS system and users.

Currently, the DSRC regulatory requirements in many parts of the world are in the process of being finalised. It is important that similar spectrum allocation and requirements will be adopted worldwide for DSRC applications [4]. The frequency bands known so far in Europe and USA are shown in Figure 2.

It is recognised that the frequency spectrum dedicated for road safety applications in Europe is 30MHz (channels 176, 178, and 180), in comparison with USA band allocation where the frequency spectrum for this application is limited to 10MHz (channel 184).

The channel number (CN) is derived by counting the number of 5MHz spectrum in the frequency band from 5000 MHz to the centre frequency *f* (CN) of the channel CN, i.e.

$$f(CN) = 5000 + 5CN\ (MHz) \qquad (1)$$

The transmitter power of a DSRC unit is described by defining four classes of devices whose maximum transmission (TX) power ranges from 0dBm to 28.8dBm. The corresponding coverage distance by a single radio link depends on the channel environment, the TX power and the modulation and coding schemes (MCS) used. This distance may range from 10m to 1km.

### 3.2 Long Term Evolution for V2X (LTE-V)

Recent studies have preferred using LTE-V as the V2X technology, mainly because LTE cellular network infrastructure already exists. LTE-V, also known as LTE Vehicular, is a variant of LTE that has been standardised by 3GPP in its most recent major standards update, Release 14 [9]. LTE-V technology is considered to be one of the optimal choices for effective ITS communications solution mainly because of its low cost of deployment since it can fully utilise existing base stations around the world. However, LTE-V is still in its study phase in 3GPP, and it became a Work Item in 3GPP Release 14 for formal standardisation. Once the standard is finalised, it is likely to take at least one year to produce a commercial chipset. Therefore, LTE-V is unlikely to be available for commercial application until late 2018 or beyond.

The frequency bands used for LTE are described in a number of standards such as [10] and [11], however, spectrum harmonisation is required for global inter-operability and implementation of low-cost V2X services. Some of the main parameters of DSRC and LTE-V networks are summarised in Table 1.

| Characteristics | IEEE 802.11p | LTE-V |
|---|---|---|
| Coverage | Intermittent | Ubiquitous |
| Capacity | Medium | High |
| Mobility | Medium | Very high |
| Network infrastructure | Huge investment | Existing network for V2I |
| Frequency bands | 5.9GHz ISM band | 3G,4G bands |
| Bit rate | Up to 27Mbps | Up to 2Mbps |

Table 1: Comparisons between DSRC/WAVE and LTE-V

### 3.3 Organisations and consortiums

Modern V2X communications are using multiple overlapping ad-hoc networks to operate with very high quality of service. They have to fulfil the requirements of the automotive applications in an extreme multipath environment (reflections, high speed of the vehicles, dynamic traffic scenarios, etc.). In order to solve those problems, several standardisation authorities have developed new standards and recommendations.

The **European Telecommunications Standards Institute** (ETSI) produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies.

The **Institute of Electrical and Electronics Engineers Standards Association** (IEEE-SA) is an organisation within Institute of Electrical and Electronics Engineers (IEEE) that nurtures, develops and advances global standards in a broad range of industries. The IEEE-SA developed 802.11p, an amendment to the IEEE 802.11 standard, to support wireless access in vehicular environments (WAVE). They define enhancements to 802.11 that are the basis of products marketed as Wi-Fi required to support specificities of ITS applications.

Standards from **Society of Automotive Engineers** (SAE) are used to advance mobility engineering throughout the world. Their standards are internationally recognised for their role in helping ensure the safety, quality, and effectiveness of products and services across the mobility engineering industry.

The **International Telecommunication Union** (ITU) is the United Nations specialised agency for information and communication technologies (ICT). The Study Groups of ITU's Telecommunication Standardisation Sector (ITU-T) assemble experts from around the world to develop international standards known as ITU-T Recommendations which act as defining elements in the global infrastructure of ICT.

The **International Organisation for Standardisation** (ISO) is an independent, non-governmental international organisation with a membership of 163 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.

The ITS station reference architecture proposed by ISO is shown in Figure 3.

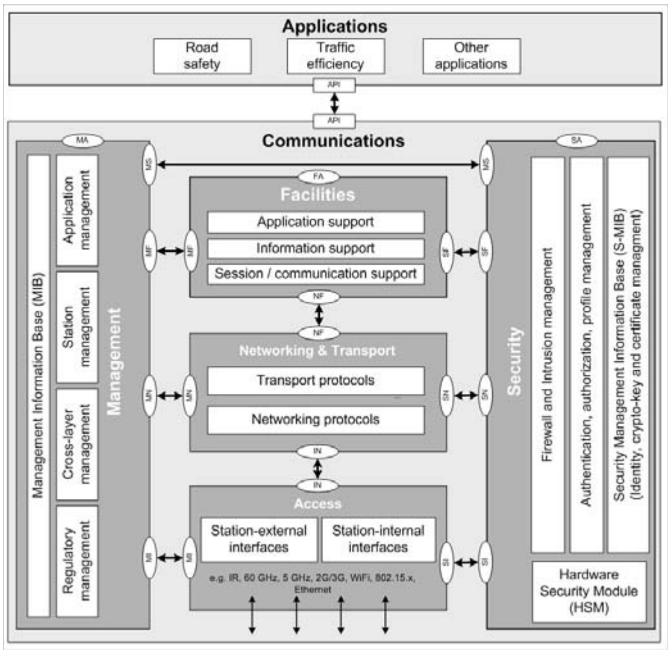

Applications
Road safety
Traffic efficiency
Other applications
API
API
Communications
MA
SA
MS
MS
FA
Facilities
Application support
Information support
Session / communication support
MF
MF
SF
SF
NF
NF
Networking & Transport
Transport protocols
Networking protocols
MN
MN
SN
SN
IN
IN
Access
Station-external interfaces
Station-internal interfaces
e.g. IR, 60 GHz, 5 GHz, 2G/3G, WiFi, 802.15.x, Ethernet
MI
MI
SI
SI
Management Information Base (MIB)
Application management
Station management
Cross-layer management
Regulatory management
Management
Security
Firewall and Intrusion management
Authentication, authorization, profile management
Security Management Information Base (S-MIB) (Identity, crypto-key and certificate managment)
Hardware Security Module (HSM)

Figure 3: The ITS station reference architecture originally developed for CALM

The **CAR 2 CAR Communication Consortium** (C2C-CC) is a non-profit, industry driven organisation initiated by European vehicle manufacturers and supported by equipment suppliers, research organisations and other partners. It supports the creation of European standards for communicating vehicles spanning all brands. As a key contributor the C2C-CC works in close cooperation with the European and international standardisation organisations. In cooperation with infrastructure stakeholders the C2C-CC promotes the joint deployment of cooperative ITS. The vehicle manufacturers, such as Volkswagen, BMW, Renault, Audi, Volvo, Daimler and the Peugeot Citroen group, have been joined by 17 technology suppliers, such as Swarco, Continental, NEC, Bosch and Denso Corporation, plus 30 academic institutions and research organisations.

## 4 Cyber Security Standardisation in V2X

There are two Harmonisation Task Groups (HTG) established by the EU-US International Standards Harmonisation Working Group: HTG1 to harmonise standards (including ISO, CEN, ETSI, IEEE) on security to promote cooperative ITS interoperability; and HTG3 to harmonise communications protocols. In collaboration, the two HTGs developed integrated set of technical reports including the report published by HTG1 that provides feedback for Standards Development Organisations and identifies areas where policy or regulatory action can help improve security [11].

CEN and ETSI are currently developing work items on serviceID (application identifier). Their goal is to harmonise serviceIDs globally (CEN, ETSI, ISO, IEEE, etc.) and to specify the management of the numbers (registration authority, etc.). ETSI STF 404 currently is doing the first step, i.e. developing a harmonised scheme (CEN, ETSI, ISO, IEEE) for serviceID.

A list of security and privacy standards for ITS developed by ETSI are shown in Table 2.

| Standard title | Standard number |
|---|---|
| Threat, Vulnerability and Risk Analysis (TVRA) | ETSI TR 102 893 |
| Stage 3 mapping for IEEE 1609.2 | ETSI TS 102 867 |
| Confidentiality services | ETSI TS 102 943 |
| Trust and Privacy Management | ETSI TS 102 941 |
| Access Control | ETSI TS 102 942 |
| ITS communications security architecture and security management | ETSI TS 102 940 |
| Security header and certificate formats | ETSI TS 103 097 |

Table 2: Base standards for security and privacy in ITS developed by ETSI

### 4.1 Security architecture

The set of CALM communication standards is built on the basis of the well-known layered OSI model, which was simplified and extended in order to define the ITS station reference architecture ISO-21217, which consists of six parts (Applications, Management, Access, Networking & Transport, Facilities and Security) (see Figure 3)

Although security has been described as a vertical layer adjacent to each of the ITS layers in [8] in ETSI Technical Specifications for ITS communications security architecture and security management [12] security services are provided on a layer-by-layer basis.

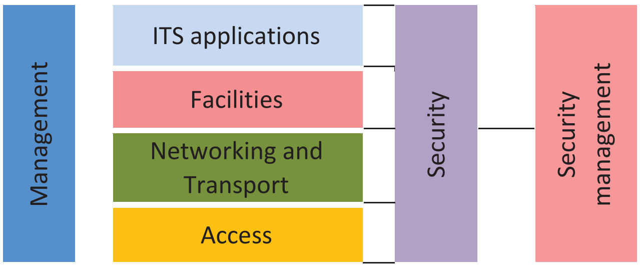


Figure 4: Architectural ITS security layers defined in [12]

### 4.2 Identity and Access Management (IdAM) frameworks for ITS

In practice, cryptographic algorithms are used to provide the V2X ITS security requirements. These algorithms rely on symmetric or asymmetric keys. To use asymmetric keys, a ITS station has to contact a trusted Certification Authority (CA) to get a certificate. A number of different PKI infrastructures have been proposed for ITS architecture.

The ETSI PKI architecture specified in [13] lists security services for ITS stations, including enrolment services, authorisation services, integrity services and plausibility validation services (see Figure 5).

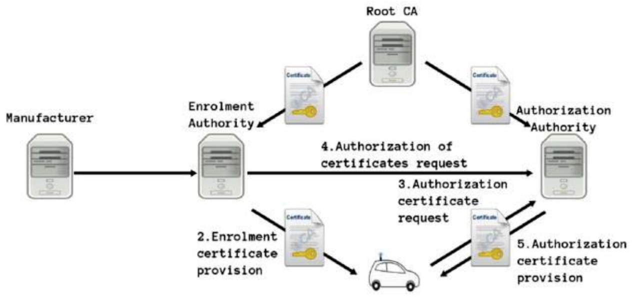

Root CA
Manufacturer
Enrolment Authority
Authorization Authority
4.Authorization of certificates request
3.Authorization certificate request
2.Enrolment certificate provision
5.Authorization certificate provision

Figure 5: ETSI ITS PKI Architecture [12]

In order to satisfy all the communications security services requirements, several elements within their functional model are proposed.

An Enrolment Authority (EA) issues a proof of identity to ITS-S identifier by delivering an enrolment certificate and then the station requests its authorisation certificates from an Authorisation Authority (AA) using the received enrolment credentials. AA verifies ITS-S enrolment credentials with EA before responding with authorisation certificates.

## 5 Security attacks in V2X communications

Threat analyses of V2X communications have been conducted in various ITS projects [14], [15] and standardisation activities [16], [17]. Based on the attack surfaces defined in state-of-the-art we summarise three access perimeters which may be considered separately because of their specific characteristics (see Figure 6) or namely (1) Infrastructure domain; (2) V2X domain; and (3) In-vehicle domain.

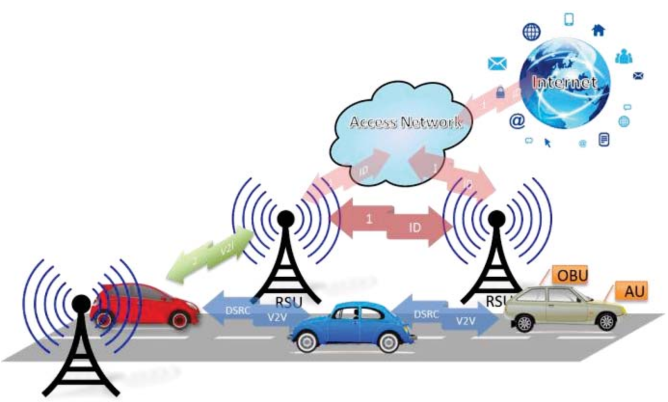


Figure 6: Simplified view of ITS environment presenting three of the main access domains.

The infrastructure domain includes vehicle manufacturers (supply chain), service providers (emergency services, billing, etc.), and trust authorities (TA). Attacks applied at this domain may be platform integrity, data analysis, denial of service (DoS) against functionality, etc.

The V2X domain is representing all the V2X communications, such as the communication between vehicle on-board unit (OBU) and road-side units (RSU) as well as the communication between neighbouring vehicles (V2V) or even V2P. Types of attacks which can be applied at this domain includee: Black hole, Flooding, Sybil attack, and jamming.

The in-vehicle domain consists of the trusted platform modules (TPM), application units (AU), and electronic control units (ECU). Examples of attacks at this domain may be tampering or physically damage units, manipulating the in-vehicle communications, etc.

## 6 Conclusions and future work

V2X communications in ITS are much more vulnerable to attack than wired networks. In V2X every vehicle node can move freely within the range of the V2X network and stay connected. Further, each fixed node (e.g. RSU) can communicate with other nodes, vehicular or fixed, in either a single hop or multi hop. In future, it is possible that authentication schemes may be enhanced by using neural network associative memories to augment or replace traditional authentication schemes.

It is currently under discussion whether Internet Protocol (IP)v6 is the only way to globally address future cars [18]. For safety messages normal IP has too large overhead, a CAM or DENM V2V message is much more compact and IP cannot compete with them. It has direct influence to the message transmission times.

In many ways there is a fundamental issue with privacy regarding the location and nature of V2V information processing. Much of the ITS communications development work is based on data being sent to and processed in the cloud, which can increase the privacy risk. An alternative model would involve more data being processed on the vehicle in relation to its immediate surroundings.

## 7 Acknowledgements

This work is conducted under an international technology R&D collaboration program that is supported by the Ministry of Trade, Industry & Energy (MOTIE) and Korea Institute for Advancement of Technology (KIAT) (N0001710).

## References

[1] E. Hamida, H. Noura, and W. Znaidi, “Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures,” *Electronics*, vol. 4, no. 3, pp. 380–

423, 2015.

[2] C. Maple, “Security and privacy in the internet of things,” *J. Cyber Policy*, vol. 2, no. 2, pp. 155–184, 2017.

[3] M. Wolf, M. Scheibel, and T. Ü. V. I. Gmbh, “A Systematic Approach to a Quantified Security Risk Analysis for Vehicular IT Systems,” *ESCRYPT Automot. Saf. Secur.*, pp. 195–210, 2012.

[4] Y. J. Li, “An Overview of the DSRC / WAVE Technology,” *Qual. Reliab. Secur. Robustness Heterog. Networks*, pp. 544–558, 2012.

[5] S. Bharati and W. Zhuang, “CAH-MAC: Cooperative ADHOC MAC for vehicular networks,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 470–479, 2013.

[6] K. Bilstrup, “Does the 802.11p MAC Method Provide Predictable Support for Low Delay Communications?,” *Sophia*, pp. 1–17, 2009.

[7] IEEE, *IEEE Standard for Information Technology — Telecommunications and Information Exchange Between Systems — Local and Metropolitan Area Networks — Specific Requirements*, vol. 2007, no. June. 2007.

[8] ETSI EN 302 665, “Intelligent Transport Systems (ITS); Communications Architecture,” *ETSI Stand.*, vol. 1, pp. 1–44, 2010.

[9] 3GPP TR 22.885, “Study on LTE support for Vehicle to Everything (V2X) services,” 2015.

[10] ETSI 3GPP TS 136 211, “Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation,” 2011.

[11] ETSI 3GPP TS 136 213, “Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures,” 2014.

[12] S. Cadzow, W. Hoefs, F. Kargl, R. Roy, S. Sill, and W. Whyte, “EU-US Standards Harmonization Task Group Report : Feedback to Standards Development Organizations — Security,” p. 58, 2012.

[13] ETSI TS 102 940, “ITS communications security architecture and security management,” *Tech. Specif.*, vol. 1, pp. 1–29, 2012.

[14] S. S. A. Festag, G. Noecker, M. Strassberger, A. Lübke, B. Bochow, M. Torrent-moreno, “NoW – Network on Wheels. Project Objectives, Technology and Achievements,” *Proc. 5th Int. Work. Intell. Transp.*, vol. 5, no. March, pp. 211–216, 2008.

[15] Preserve Consortium, “Preparing Secure V2X Communications,” 2015. [Online]. Available: http://www.preserve-project.eu.

[16] ETSI TR 102 893, “ITS; Security; Threat, Vulnerability and Risk Analysis (TVRA),” *Intell. Transp. Syst.*, vol. 1, pp. 1–86, 2010.

[17] SAE J3061, “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems,” 2016.

[18] ITSSv6, “ITSSv6 Deliverable D2 . 1 Preliminary System Recommendations,” 2012.