A Preliminary Security Assessment of 5G V2X

Citation for the original published paper (version of record):
Lautenbach, A., Nowdehi, N., Olovsson, T. et al (2019). A Preliminary Security Assessment of 5G V2X. IEEE Vehicular Technology Conference, 2019-April.
http://dx.doi.org/10.1109/VTCSpring.2019.8746547

A Preliminary Security Assessment of 5G V2X

Aljoscha Lautenbach*†, Nasser Nowdehi*‡, Tomas Olovsson* and Romi Zaragatzky§
* Chalmers University of Technology, SE-412 96 Gothenburg, Sweden
{aljoscha,nasser.nowdehi,tomas.olovsson}@chalmers.se
† Evidente AB, SE-411 03 Gothenburg, Sweden
‡ Volvo Car Corporation, SE-405 31 Gothenburg, Sweden
§ AB Volvo, SE-405 08 Gothenburg, Sweden
romi.zaragatzky@volvo.com

***Abstract*—This is the authors' version of this paper. The final authenticated version is copyrighted by IEEE and is available online at https://www.doi.org/10.1109/VTCSpring.2019.8746547.**

Research on intelligent transport systems (ITS) for improved traffic safety and efficiency has reached a high level of maturity and first applications will hit the market in 2019. Since 2004, the wireless standard 802.11p has been developed specifically for ITS services. Since then new telecommunication standards have been devised, and the new 5G telecommunication standard is nearing completion. Due to its technological advantages such as higher speeds and reliability, it is being considered to be used for ITS services. The new radio technology "New Radio (NR)", which is being developed as part of 5G, can complement or replace 802.11p in V2X applications. While there has been some work to compare 802.11p and 5G New Radio in terms of performance and applicability for safety-critical use cases, little work has been done to investigate the implications for security. In this paper, we provide an overview of the security requirements of known ETSI ITS use cases, and based on those use cases we compare and assess the security implications of replacing 802.11p with cellular V2X. We find that due to the use of millimeter waves, beamforming and massive MIMO, there will be an implicit improvement for confidentiality and privacy, and it may also be possible to shorten authentication procedures in certain cases. When a fully network-assisted C-V2X mode is chosen, it is also possible to outsource several of the ITS security requirements to the cellular network.

***Index Terms*—Security, 5G, ITS, V2X, ETSI, VANET, 802.11p, New Radio**

I. Introduction

Cooperative Intelligent Transport Systems (C-ITS) aim at improving road safety and traffic efficiency while also reducing environmental impact. They achieve this by enabling vehicles and roadside infrastructures to communicate and exchange safety-relevant messages. These messages contain information such as road hazards, speed, location, size, and direction of ITS nodes and are sent over Vehicular Ad-hoc Networks (VANETs). VANETs enable vehicles and responsible authorities to distribute traffic information and safety relevant warnings.

In Europe, the European Telecommunication Standards Institute (ETSI) has introduced the ETSI ITS G5 (ITSC) standard [1] to enable the implementation of so called Vehicle-to-Anything (V2X) communication. The ITSC standard is based on IEEE 802.11p with some amendments towards European requirements. This standard enables dedicated short range communications between vehicles and Road Side Units (RSUs), and its effective range of application is up to 500 meters [2]. Moreover, it defines a communication architecture and a standardized set of services and interfaces that enable secure V2X communications.

In addition to the 802.11p based V2X standard, the 3rd Generation Partnership Project (3GPP), which is responsible for many telecommunication standards and projects, has investigated the possibility of using the Advanced Long Term Evolution (Advanced LTE) cellular network for V2X communications. 3GPP and ETSI collaborated to develop standards to enhance LTE communications for V2X applications [3, 4]. The new telecommunication standard under development, 5G, and the related new radio technology "New Radio (NR)" promise significant improvements w.r.t network latency, throughput and reliability in V2X communications. The development and standardization of 5G for V2X communications is ongoing and the 5G Automotive Associations (5GAA) is developing 5G enabled solutions for V2X applications [5].

Although V2X communications offer safety and environmental benefits, there are also security and privacy concerns. The V2X messages exchanged between ITS users often contain data such as speed, direction and GPS coordinates. Therefore, it must be ensured that V2X messages cannot be linked to individuals. Furthermore, due to their safety-critical nature, ITS messages should be protected against tampering and injection of data by unauthorized entities, which can mislead the drivers and lead to road accidents or redirecting traffic flow. In particular, ETSI has introduced a security architecture that offers pseudonymity, confidentiality, authenticity and integrity services by using certificate authorities and identity management procedures.

Since the 802.11p protocol itself does not provide any mechanisms for authenticating ITS users for performance reasons, ETSI ITSC addresses security and privacy concerns with services in the higher layers of the communication stack. In this paper we consider whether 5G V2X can facilitate security features at lower levels, and what the security impact of replacing 802.11p with 5G NR in the ETSI stack would be. Our contributions are that we (1) analyze the security requirements of ETSI ITS use cases, (2) investigate the properties of 5G NR that can be used for physical layer security and (3) explore the security implications of using 5G V2X for the

ETSI ITS use cases.

II. Related Work

We will shortly present some related work to put our work into context. Filippi et al. [6] compare 802.11p and 5G for V2X applications, but they focus exclusively on safety. Similarly, Vukadinovic et al. [7] compare the two technologies for the particular V2X use case "platooning", once again with a focus on safety and performance. Bian et al. [8] on the other hand provide an overview of the security in V2X use cases. Gupta and Jha [9] and Agiwal et al. [10] present surveys of emerging 5G technologies, while Shah et al. [11] discuss the building blocks of 5G which are of interest for V2X applications. Finally, Ahmad et al. [12] provide an overview of 5G security from an architectural perspective.

III. V2X Communication

Currently, there are two underlying technologies that enable V2X communication, namely IEEE 802.11p and cellular technologies. In this section, we first describe different communication scenarios in V2X communication, and then explain how 802.11p based V2X and Cellular V2X (C-V2X) technologies enable these scenarios to support a set of ITS applications.

A. V2X Communication Scenarios

V2X communication has several components including Vehicle-to-Vehicle (V2V), Vehicle-to-Roadside Unit (V2R) and Vehicle-to-Network (V2N) communications. V2N communication always has to go through a base station (BS) or an RSU, but for V2V and V2R different communication scenarios exist depending on the underlying V2X technology. We distinguish three general types of communication scenarios: direct communication, fully-network assisted and semi network-assisted communication.

In *direct communication*, vehicles and RSUs are able to exchange messages without the need to establish a connection to network infrastructure prior to data exchange. This is the only supported mode for the comparatively low data transmission rate technology 802.11p, in order to be able to fulfill the low-latency and high-reliability requirements of safety related messages. Through the addition of a special interface called PC5, cellular based V2X nodes are also capable of direct communication without network assistance (Figure 1a). In a *fully network-assisted* scenario, which is the traditional cellular use-case, all communication has to go through the base station (BS) (Figure 1b). In a *semi network-assisted* scenario, vehicles and RSUs may use a combination of direct communication and network-assisted communication thus effectively extending the range of V2X applications (Figure 1c).

B. 802.11p Based V2X

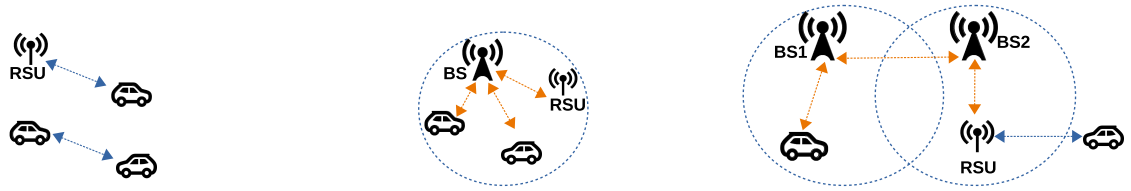
V2X communications based on 802.11p radio technology have been standardized by ETSI to enable dedicated short-range communications in the unlicensed 5.9 GHZ band. ETSI has provided several standards for ITSC that describe the Basic Set of Applications (BSA) [13], the communication architecture [14], the protocol stack [15, 16], the messages [17, 18], and the security requirements, services and architecture [19, 20, 21, 22]. In these standards, the end nodes are called *ITS station*s. The **Cooperative Awareness Message** (CAM) and **Decentralized Environmental Notification Message** (DENM) are two fundamental message types exchanged between ITS stations. These messages may contain sensitive data such as speed, location, dynamics and attributes of ITS stations.

As stated by ETSI, it must be ensured that ITSC messages do not leak any personally identifying information (e.g., location or identity of the ITS station) to any unauthorized parties [21]. Furthermore, ITS stations should be trusted before being granted specific services and applications that require authorization (e.g., claim priority rights for emergency vehicles). In order to address these security and privacy requirements, ETSI has introduced a security architecture that provides pseudonymity, confidentiality, authenticity and integrity which is achieved by using certificates, security headers and trailers (SecuredMessage), security profiles and identity management services. ETSI has also introduced a hierarchy of Certificate Authorities (CAs) [20] that are responsible for issuing and revoking different types of digital certificates. These certificates enable the ITS stations to authenticate and authorize their ITS messages without revealing their identity.

C. Cellular V2X

In 2016, the mobile industry body 3GPP standardized the use of LTE networks as an underlying technology for V2X communication in Release 14 [23]. LTE-V2X benefits from the wide coverage, broad bandwidth and long transmission range of already established cellular networks. In addition to the *Direct* communication (V2V, V2R) in the 5.9 GHZ spectrum band (Figure 1a), C-V2X enables vehicles and roadside units to exchange messages over the commercially-licensed cellular spectrum through a V2X application server (V2N). In the Direct mode, which is typically referred to as Device to Device (D2D) mode, vehicles and roadside units communicate over Sidelink channels using a PC5 radio interface without relying on the cellular network to send the traffic [24]. The C-V2X standard is compatible with both 4G and 5G and the introduction and deployment of 5G networks will enhance C-V2X by enabling precise positioning, high throughput, high reliability and low latency data transmission.

The 3GPP consortium has identified security and privacy requirements [3], where C-V2X users shall be authenticated before employing the cellular network for V2X communication, and the integrity of the transmitted data shall be protected by measures provided by the network. Moreover, for sensitive V2X services and sensitive data such as cryptographic keys in transition or at rest, the confidentiality of message content shall be protected. Also, the pseudonymity and privacy of V2X users shall be protected, by ensuring that the user's identity cannot be tracked or identified by any other V2X user, nor by any single party (operator or third party). Although V2N communication in cellular based V2X is protected by the



(a) Direct communication (802.11p or PC5)

(b) Fully network-assisted (4G/5G)

(c) Semi network-assisted (4G/5G + 802.11p or PC5)

Fig. 1: Different scenarios for V2V and V2R communications

existing cellular network Authentication and Key Agreement (AKA) protocol, direct communications between vehicles and RSUs may rely on the security mechanisms provided by other standards (e.g. ITSC) [25].

D. Basic Set of Applications

ETSI [13] has identified four major V2X application classes, namely Active Road Safety, Cooperative Traffic Efficiency, Cooperative Local Services and Global Internet Services. Each application class is further divided into smaller applications, where each application consists of several use cases. The **Active Road Safety** applications focus on informing the surrounding vehicles about hazardous incidents on the road such as *roadwork* or *collision risk warning*, and drivers' potentially dangerous behavior such as *lane change* and *overtaking*. The **Cooperative Traffic Efficiency** applications aim at optimizing the traffic efficiency by enabling vehicles and infrastructures to exchange messages related to speed management and cooperative navigation. The **Cooperative Local Services** group consists of location based services that enable RSUs to deliver local services such as *access control* and *parking management* to passing vehicles. The **Global Internet Services** allow vehicles and RSUs to connect to the Internet and enable services such as *fleet management*, *stolen vehicle alert*, *vehicle software/data provisioning* and *instant messaging*.

IV. Security Requirements of ETSI ITS Use Cases

In order to assess the impact of introducing 5G NR in V2X communications, we detail the security requirements for ITS applications and base our assessment on these requirements. As outlined in section III-D, there are four main ETSI ITS application classes that consist of different use cases [13], which have different security requirements. In this Section, we present and motivate these requirements and provide an in-depth analysis of different application use cases. For each use case, we study the requirements w.r.t security attributes identified by ETSI, which are *confidentiality*, *integrity*, *availability*, *privacy* and *authentication*. The results of our analysis are summarized in Table I.

A. Active Road Safety

The Active Road Safety use cases are safety-critical, thus they have high reliability and real-time requirements in order to be shown to the driver as soon as possible.

***Confidentiality*:** Given that all vehicles and relevant road side units have to be capable of receiving and processing the cooperative awareness messages and road hazard warnings, the ETSI ITS standard has not specified *confidentiality* requirements for this class of use cases. Furthermore, the messages that enable these use cases do not carry any sensitive data that require *confidentiality*.

***Integrity*:** The information exchanged in Active Road Safety messages are safety-critical, thus they have to be protected against modifications. Therefore, this class of use cases have strict *integrity* requirements.

***Availability*:** This class of use cases have strict *availability* requirements due to their high reliability and real-time requirements.

***Authentication*:** In all Active Road Safety use cases the receiver has to verify whether the sender of the message is a trustable (authorized) ITS station.

***Privacy*:** Some of the Active Road Safety use cases are based on messages broadcasted by RSUs (e.g. Roadwork warning and Signal violation warning) that do not contain privacy sensitive information. However, most of road safety use cases are based on messages broadcasted by vehicles (e.g. Slow vehicle indication)which contain privacy sensitive data such as vehicle's current location and direction. An attacker should not be able to link such information collected from disperse locations and times to a vehicle. Therefore, *privacy* is a concern for this class of applications.

B. Cooperative Traffic Efficiency

The Cooperative Traffic Efficiency use cases are enabled by permanently broadcasting authoritative messages triggered by traffic management entities, to enhance traffic efficiency and reduce the pollution created by vehicles. Although this application class is not safety-critical, misuse of its use cases can potentially lead to traffic incidents.

***Confidentiality*:** The Cooperative Traffic Efficiency messages are broadcasted to all ITS stations within a certain geographical area and do not contain sensitive information that require *confidentiality*.

***Integrity*:** Although the *integrity* of the messages that carry traffic information should be verified by the receivers, the exchanged messages are not as safety-critical as the Active Road Safety messages.

Applications Class	Application	Use case	V2X	Conf.	Integ.	Avail.	Authen.	Priv.
Active Road Safety	Driving Assistance - Cooperative Awareness	Emergency vehicle warning	V	0	2	2	2	2
		Slow vehicle indication	V	0	2	2	2	2
		Intersection collision warning	VR	0	2	2	2	2
		Overtaking vehicle warning	V	0	2	2	2	2
		Lane change	V	0	2	2	2	2
		Glare reduction	V	0	2	2	2	2
		Motorcycle approaching indicator	VR	0	2	2	2	2
	Driving Assistance - Road Hazard Warning	Emergency electronic brake lights	VRN	0	2	2	2	2
		Stationary vehicle	VRN	0	2	2	2	2
		Wrong way driving warning	VRN	0	2	2	2	1
		Traffic condition warning	VRN	0	2	2	2	1
		Signal violation warning	R	0	2	2	2	0
		Roadwork warning	VR	0	2	2	2	0
		Collision risk warning	VR	0	2	2	2	1
		Collision unavoidable	VR	0	2	2	2	1
		Decentralized floating car data	VRN	0	2	2	2	1
Cooperative Traffic Efficiency	Speed Management	Regulatory / contextual speed limits notification	RN	0	2	1	2	0
		Traffic light optimal speed advisory	R	0	2	1	2	0
	Cooperative Navigation	Traffic information and recommended itinerary	R	0	2	1	2	0
		Enhanced route guidance and navigation	RN	0	2	1	2	0
		Limited access warning and detour notification	R	0	2	1	2	0
		In-vehicle signage	R	0	2	1	2	0
		Point of Interest notification	R	0	2	1	2	0
Cooperative Local Services	Location Based Services	Automatic access control and parking management	RN	2	2	1	2	2
		Local electronic commerce	RN	2	2	1	2	2
		Media downloading	RN	2	2	1	2	2
Global Internet Services	Communities Services	Insurance/financial services	RN	2	2	1	2	2
		Fleet management	RN	2	2	1	2	2
		Loading zone management	RN	2	2	1	2	2
	ITS Station Life Cycle Management	Vehicle software/data provisioning and update	RN	2	2	2	2	2
		Vehicle-RSU sensor data calibration	RN	0	2	1	2	0

TABLE I: ITS use cases and their security requirements: 0 = not required, 1 = intermediate, 2 = strict

***Availability*:** These use cases are less time critical than the Active Road Safety applications. Thus, they do not have high *availability* requirements.

***Authentication*:** For all use cases in this application class, the receivers have to verify the authenticity of the RSU that disseminates the traffic information. Moreover, the receivers have to verify whether the RSU is authorized to send traffic advisory messages.

***Privacy*:** All use cases in this application class are based on privacy-insensitive messages sent by RSUs.

C. Cooperative Local Services and Global Internet Services

These two classes of applications aim at advertising and providing on-demand commercial or non-commercial information to passing vehicles. Global Internet Services rely on service providers on the Internet and relay ITS messages to the Internet, while the Cooperative Local Services are enabled by the services provided from within the ITS network infrastructure.

***Confidentiality*, *Integrity*, *Authentication* and *Privacy*:** Almost all use cases in these applications have high requirements for *confidentiality*, *integrity*, *authentication* and *privacy*. This is mainly because the exchanged ITS messages may carry sensitive information (e.g. financial or insurance information) that are only meant to be shared with authorized entities, or privacy sensitive information such as vehicle parameters, vehicle type, geographical position and delivery time that can be used to associate ITS identities to individuals. The only exceptions are the Point of interest notification and Vehicle and RSU sensor data calibration services that do not exchange messages with personal or confidential content.

***Availability*:** None of these use cases has high *availability* and real-time requirements as the they are not safety critical.

Overall, it can be noted from Table I, that the use cases with safety impacts require *integrity*, *availability*, *authentication* and *privacy*, while *confidentiality* do not seem to be a major concern. On the other hand, use cases that rely on communications with external entities on the Internet have high *confidentiality* requirements.

V. Security Implications of using 5G NR in V2X Applications

In order to investigate to which degree V2X security mechanisms can be simplified or removed from higher layers when C-V2X and 5G are used, we consider the new physical layer of 5G, a technology simply called New Radio (NR). Release 15 of 3GPP, which has a first full specification of NR, was published in June 2018. Further improvements to 5G are expected in the future release 16, and several researchers have proposed security enhancements that might be of interest.

A. 5G New Radio (NR) and Physical Layer Security

NR is being developed for various communication needs and is expected to provide faster and more reliable communication. The key applications that have been identified by the International Telecommunication Union (ITU) for 5G are enhanced mobile broadband (eMBB), ultra-reliable and low-latency communications (URLLC), and massive machine type

communications (mMTC) [26]. The resulting target requirements are significant improvements over older technology. For instance, the peak data rate should be 20 Gbit/s and the user plane latency should be below 1 ms for URLLC applications such as V2X applications. In order to fulfill these requirements, several new technologies are being utilized for NR, including millimeter waves (mmWave), beamforming and massive multiple-input multiple-output (MIMO). In addition to the performance and reliability advantages, these technologies also offer new possibilities for physical layer security.

The idea of **physical layer security (PLS)** for wireless networks based on information theoretic security [27] has been around since 1975 [28], but in the last two decades the ideas have become more practical [29, 30]. The underlying idea is to use physical properties of the transmission medium[1] to secure a channel which avoids the overhead of cryptography [30, 31]. Many of these ideas apply to wireless communication in general, but there are some PLS mechanisms that apply specifically to the technologies used by 5G NR.

One security concern in wireless communication is **authenticity**. As long as the environment is sufficiently stable, a wireless channel has a unique fingerprint of physical properties that identifies it, which can be used to authenticate a previously established connection [31, 32, 33]. This essentially allows authentication based on sender/receiver *location*, because if the location or the environment changes significantly, the physical channel fingerprint will change as well. This assumption may not hold in vehicular networks where communicating nodes move at high speeds [31, 32], but Al-Momani et al. [32] argue that due to the high frequency of messages their method of re-authentication may still be of use. The idea is to establish initial authenticity via cryptographic means, but to skip the cryptographic authentication of following messages as long as the physical fingerprint matches.

1) Millimeter Waves and Beamforming: Millimeter wave technology can provide higher data transmission rates and broader bandwidth by using a wavelength of 1 - 10 mm (with carrier waves between 30 and 300 GHz), thus allowing for much smaller antennas [34, 35]. The short wavelength introduces some new challenges such as sensitivity to weather conditions and blocking objects, and a shorter maximum range ($\sim$1 km). However, the small antenna size enables the use of multiple antennas to overcome those challenges with narrowly focused beams. This beamforming is achieved by utilizing the antennas in such a way that there is constructive interference in the desired signal direction and destructive interference in all other directions. This can increase the signal strength and thus the effective range significantly. Using beamforming in V2X applications is rather challenging due to the fast moving communicating nodes. Tracking algorithms offer potential solutions, and this is an active research area.

A common assumption in physical layer security is that the high directionality achieved with narrow beams implies **confidentiality** and **privacy**, because a potential eavesdropper would have to move to intercept. However, Steinmetzer et al. [36] found that narrow beams offer less protection than commonly assumed, because small objects can reflect the beam strongly enough to eavesdrop. Nevertheless, eavesdropping is harder when narrow beams are used [31, 37].

2) Massive MIMO: The idea of multiple-input-multiple-output (MIMO) systems is to use multiple antennas on the transmitting and receiving end to exploit multipath propagation to increase channel capacity. Multipath propagation describes the effect that, due to reflecting objects in typical indoor or urban environments, there are several paths a radio wave can take. If not accounted for, multipath propagation leads to channel fading, but if utilized properly for spatial diversity (same signal, different paths) and spatial multiplexing (different signals, different paths) with multiple antennas, it can improve the channel capacity instead [38]. Traditional MIMO systems have 2 to 8 antennas, but with the advent of millimeter waves it is possible to use many more antennas, a configuration commonly termed massive MIMO [34, 39]. Advantages of massive MIMO include increased data rate, increased signal to noise ratio, more stable and predictable channel conditions, and increased potential for physical layer security [40]. In addition to the reduced information leakage due to higher directionality, some of the antennas can also be used to transmit artificial noise to confuse eavesdroppers [31].

B. C-V2X Security for ETSI ITS Use Cases

802.11p has no security on the physical or link-layer since the performance degradation was considered too costly. Cellular V2X offers an alternative to 802.11p, and with the significantly improved performance of 5G NR it might be worth to reconsider physical layer security. The initial releases of C-V2X referred to LTE only, but newer versions integrate with 5G. While the use of 5G new radio in all V2X communication scenarios is a long term goal, at the moment the technology can only be fully utilized on base stations or roadside units. There are still several open research questions before 5G NR can be deployed on vehicles. This is why only LTE can be used for direct sidelink communication via PC5 (see Figure 1a) in the near future, but 5G NR can be used in network-assisted scenarios (see Figures 1b and 1c). In the following we assess which of the security requirements of the ETSI ITS use cases (see Table I) could be handled by lower layers when C-V2X and 5G NR are used. Since the security that can be offered depends heavily on the type of communication (direct communication vs network-assisted), we discuss those types separately. However, for direct communication and semi network-assisted communication the same argument applies for all use cases, so we group them here for all use cases:

Direct Communication (V2V, V2R): Since 5G NR can not be used for direct communication yet and LTE network security can also not be used (no network coverage), there are no security advantages.

Semi-Assisted Network (V2V, V2R, V2N): For the direct communication part, the argument above applies, and for the

[1] typically channel state information (CSI)

network-assisted parts, the argument for the fully network-assisted part below applies.

1) Active Road Safety: Due to their safety-critical nature, all of the applications in the active road safety class have strict requirements for integrity, availability and authenticity. About half of the use cases also have strong privacy requirements.

Fully network-assisted (V2V, V2R, V2N): If all communication goes over a cellular base station, integrity and authenticity are implicitly covered by LTE or 5G, because all messages are signed and encrypted. Privacy is partly covered through the encryption, but the nature of privacy is slightly more complex: the identity of the sender should not be revealed. Therefore, the use of temporary identities is important. When 5G NR is being used, re-authentication via the physical layer could also be considered to speed up the process, and the highly directional communication increases privacy.

2) Cooperative Traffic Efficiency: Since applications for cooperative traffic efficiency are not about individual drivers, there are no privacy or confidentiality concerns. However, malicious manipulation of such messages could have negative safety consequences, so message integrity and authenticity must be ensured. The availability requirements are not strict since a lost message has no serious consequences.

Fully network-assisted (V2V, V2R, V2N): Once again, integrity and authenticity are implicitly covered by LTE or 5G, and re-authentication via the physical layer might be possible.

3) Cooperative Local Services and Global Internet Services: The most stringent security requirements apply to cooperative local services and global internet services, since most of them involve transactions for individual users. Once again, since the applications are not safety-critical, availability is not a major concern, with the exception of software updates which may have safety and security implications.

Fully network-assisted (V2V, V2R, V2N): Once again, integrity, authenticity and confidentiality are implicitly covered by LTE or 5G, and re-authentication via the physical layer might be possible. For privacy, the same argument as for active road safety applies.

VI. Conclusion

In order to understand the security implications of using C-V2X and 5G New Radio (NR) for V2X communications, we analyze the security requirements for ETSI ITS use cases and we explore some physical layer security mechanisms that could be adopted for 5G NR.

We find that due to the use of millimeter waves, beamforming and massive MIMO, there will be an implicit improvement for confidentiality and privacy, and it may also be possible to shorten authentication procedures in certain cases. When a fully network-assisted C-V2X mode is chosen, it is also possible to outsource several of the ITS security requirements to the cellular network.

Our assessment highlights some encouraging synergies that can be achieved by bringing 5G and ITS together, and C-V2X in general seems to have a positive impact on security.

Acknowledgments

This work was partially funded by Chalmers Area of Advance Transport through the Automotive 5G Integrated Security and Communications project, and by VINNOVA, the Swedish Governmental Agency for Innovation Systems, through the project "HoliSec" (2015-06894).

References

[1] ETSI, "Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band," European Standard for Intelligent Transport Systems (ITS) TS 302 663 - V1.2.0, 2012.

[2] V. D. Khairnar and K. Kotecha, "Performance of vehicle-to-vehicle communication using ieee 802.11 p in vehicular ad-hoc network environment," *arXiv preprint arXiv:1304.3357*, 2013.

[3] ETSI, "Service requirements for V2X services," Technical specification on LTE TS 122 185 - V14.3.0 Release 14, 2017.

[4] ——, "Architecture enhancements for V2X services," Technical specification on Universal Mobile Telecommunications System (UMTS); LTE TS 123 285 - V14.3.0, 2017.

[5] "The Case for Cellular V2X for Safety and Cooperative Driving," 5G Automotive Association, Tech. Rep. 23-Nov-2016, 2016.

[6] A. Filippi, K. Moerman, V. Martinez, A. Turley, O. Haran, and R. Toledano, "IEEE802.11p ahead of LTE-V2V for safety applications," Tech. Rep., 2017.

[7] V. Vukadinovic, K. Bakowski, P. Marsch, I. D. Garcia, H. Xu, M. Sybis, P. Sroka, K. Wesolowski, D. Lister, and I. Thibault, "3GPP C-V2X and IEEE 802.11p for vehicle-to-vehicle communications in highway platooning scenarios," *Ad Hoc Networks*, vol. 74, pp. 17–29, 2018.

[8] K. Bian, G. Zhang, and L. Song, "Toward Secure Crowd Sensing in Vehicle-to-Everything Networks," *IEEE Network*, pp. 1–6, 2017.

[9] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE Access*, vol. 3, pp. 1206–1232, 2015.

[10] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016.

[11] S. A. A. Shah, E. Ahmed, M. Imran, and S. Zeadally, "5G for vehicular communications," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 111–117, Jan 2018.

[12] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," *2017 IEEE Conference on Standards for Communications and Networking, CSCN 2017*, pp. 193–199, 2017.

[13] ETSI, "Basic Set of Applications; Definitions," Technical report on Vehicular Communications TR 102 638 - V1.1.1, 2009.

[14] ——, "Communications Architecture," European standard on Intelligent Transport Systems (ITS) EN 302 665 - V1.1.1, 2010.
[15] ——, "Basic Set of Applications; Part 2 : Specification of Cooperative Awareness Basic Service," Technical specification on Vehicular Communications TS 102 637-2, 2011.
[16] ——, "GeoNetworking," Technical specification on Vehicular Communications TS 102 636-4-1 - V1.1.1, 2013.
[17] ——, "Part 3 : Specifications of Decentralized Environmental Notification Basic Service," Technical specification on Vehicular Communications TS 102 637-3, 2010.
[18] ——, "Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol," Technical specification on Vehicular Communications TS 102 636-5-1 - V1.1.1, 2011.
[19] ——, "Security; Trust and Privacy Management," Technical specification on Intelligent Transport Systems (ITS) 102 941 - V1.1.1, 2012.
[20] ——, "Security Services and Architecture," Technical specification on Intelligent Transport Systems (ITS) TS 102 731, 2010.
[21] ——, "ITS communications security architecture and security management," Technical specification on Intelligent Transport Systems (ITS) TS 102 940 - V1.1.1, 2012.
[22] ——, "Security; Security header and certificate formats," Technical specification on Intelligent Transport Systems (ITS) TS 103 097 - V1.1.1, 2013.
[23] 3GPP Release 14. http://www.3gpp.org/release-14, visited 2018-10-27.
[24] 3GPP Release 12. http://www.3gpp.org/release-12, visited 2018-10-27.
[25] 3GPP Release 15. http://www.3gpp.org/release-15, visited 2018-10-27.
[26] ITU-R, "Minimum requirements related to technical performance for IMT-2020 radio interface(s)," ITU, Tech. Rep. ITU-R M.2410-0, November 2017.
[27] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct 1949.
[28] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct 1975.
[29] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, 2011.
[30] L. Sun and Q. Du, "Physical Layer Security with Its Applications in 5G Networks : A Review," *China Communications*, pp. 1–14, 2017.
[31] Y. Liu, H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys Tutorials*, vol. 19, no. 1, pp. 347–376, Firstquarter 2017.
[32] A. Al-Momani, F. Kargl, C. Waldschmidt, S. Moser, and F. Slomka, "Wireless channel-based message authentication," in *2015 IEEE Vehicular Networking Conference (VNC)*, Dec 2015, pp. 271–274.
[33] F. Pan, Y. Jiang, H. Wen, R. Liao, and A. Xu, "Physical layer security assisted 5g network security," in *Vehicular Technology Conference (VTC-Fall), 2017 IEEE 86th*. IEEE, 2017, pp. 1–5.
[34] S. A. Busari, K. M. S. Huq, S. Mumtaz, L. Dai, and J. Rodriguez, "Millimeter-wave massive MIMO communication for future wireless systems: A survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 2, pp. 836–869, 2017.
[35] X. Wang, L. Kong, F. Kong, F. Qiu, M. Xia, S. Arnon, and G. Chen, "Millimeter wave communication: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 20, no. 3, pp. 1616–1653, thirdquarter 2018.
[36] D. Steinmetzer, J. Chen, J. Classen, E. Knightly, and M. Hollick, "Eavesdropping with periscopes: Experimental security analysis of highly directional millimeter waves," in *2015 IEEE Conference on Communications and Network Security (CNS)*, Sept 2015, pp. 335–343.
[37] C. Wang and H. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 8, pp. 5569–5585, Aug 2016.
[38] A. Goldsmith, S. A. Jafar, N. Jindal, and S. Vishwanath, "Capacity limits of mimo channels," *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 5, pp. 684–702, June 2003.
[39] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive mimo for next generation wireless systems," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 186–195, February 2014.
[40] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive mimo: An overview on passive eavesdropping and active attacks," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21–27, June 2015.