A Preliminary Security Assessment of 5G V2X

Downloaded from: https://research.chalmers.se, 2022-09-22 17:01 UTC

Citation for the original published paper (version of record):
http://dx.doi.org/10.1109/VTCSpring.2019.8746547

N.B. When citing this work, cite the original published paper.
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
† Department of Electrical and Computer Engineering, Chalmers University of Technology, SE-412 96 Gothenburg, Sweden
‡ Volvo Car Corporation, SE-405 31 Gothenburg, Sweden
§ AB Volvo, SE-405 08 Gothenburg, Sweden

Evidente AB, SE-411 03 Gothenburg, Sweden

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
We distinguish three general types of communication scenarios depending on the underlying V2X technology. Filippi et al. [6] compare 802.11p and 5G network-assisted communication. Through the addition of a special interface called PC5, cellular based V2X nodes are also capable of direct 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
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.
Communities

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Road Safety</td>
<td>Speed</td>
<td>Regulatory / contextual speed limits notification</td>
<td>RN</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td>Automatic access control and parking management</td>
<td>R</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Traffic Efficiency</td>
<td>Traffic information and recommended itinerary</td>
<td>R</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Navigation</td>
<td>In-vehicle signage</td>
<td>R</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Cooperative</td>
<td>Point of Interest notification</td>
<td>R</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Location</td>
<td>Local electronic commerce</td>
<td>R</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Based</td>
<td>Media downloading</td>
<td>R</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Services</td>
<td>Insurance/financial services</td>
<td>R</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Communities</td>
<td>Vehicle software/data provisioning and update</td>
<td>R</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Services</td>
<td>Vehicle-RSU sensor data calibration</td>
<td>R</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

**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 few decades the ideas have become more practical [29, 30]. The underlying idea is to use physical properties of the transmission medium 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] 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 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
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 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


