Security analysis of introducing 5G in V2X communications

Master's thesis in Computer Systems and Networks

ROMI ZARAGATZKY

Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
UNIVERSITY OF GOTHENBURG
Gothenburg, Sweden 2018

Master's thesis 2018

Security analysis of introducing 5G in V2X communications

ROMI ZARAGATZKY

Department of Computer Science and Engineering
Chalmers University of Technology
University of Gothenburg
Gothenburg, Sweden 2018

Security analysis of introducing 5G in V2X communications
ROMI ZARAGATZKY

Supervisor: Erland Jonsson, Department of Computer Science and Engineering
Examiner: Tomas Olovsson, Department of Computer Science and Engineering

Master's Thesis 2018
Department of Computer Science and Engineering
Division of Networks and Systems
Chalmers University of Technology and University of Gothenburg
SE-412 96 Gothenburg
Telephone +46 31 772 1000

Cover: A visualization of the future connected city.

Typeset in LaTeX
Gothenburg, Sweden 2018

Security analysis of introducing 5G in V2X communications
ROMI ZARAGATZKY
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg

Abstract

Vehicle-to-everything (V2X) communication is an area that interests many research institutions as well as the industry. The European Telecommunications Standards Institute (ETSI) has developed standards for these communications. Those standards describe a protocol stack that builds on top of the WiFi protocol 802.11p, which offers no security. With the active development of 5G, many companies and research institutes are now interested in using this new technology in V2X communications. The possibility to exchange 802.11p with 5G enables, among many other improvements, enhancing the performance of the ETSI defined security mechanisms. At the same time the new features might also bring new vulnerabilities.
The purpose of this thesis is to investigate how the introduction of 5G in V2X communications affects security. We show that the transition from 802.11p to 5G is possible but not easy, and it requires certain changes to the rest of the protocol stack. Furthermore, several possible improvements of the security mechanisms provided higher up in the stack are proposed. The improvements include removal of the current certificate mechanism for authentication, since certain features of 5G will make it redundant. Finally, the pros and cons of introducing 5G in V2X communications are discussed.

Keywords: V2X communications, 5G, 802.11p, network security, ETSI, ITS, security architecture.

Acknowledgements

I would first like to thank my thesis supervisor, Prof. Erland Jonsson, for guiding me in writing this thesis and my examiner, Assoc. Prof. Tomas Olovsson, for helping me choose the right directions in my research.
Further, I would like to thank Prof Tommy Svensson for taking time to answer my questions, and PhD. students Aljoscha Lautenbach and Nasser Nowdehi for their help and guidance. I would also like to thank Taimoor Abbas at Volvo Cars for his professional expertise.
Finally, I would like to thank my parents for helping me with my studies throughout my life and always supporting me. I would never have reached this far without their love and guidance.

Romi Zaragatzky, Gothenburg, June 2018

Contents

Abbreviations

3GPP 3rd Generation Partnership Project
5G-AKA 5G Authentication and Key Agreement
5G-PPP 5G Infrastructure Public Private Partnership
A-SU Authorized Secondary User
AIPS Another Identity-based Publish/Subscribe protocol
BSA Basic Set of Applications
BSS Basic Service Set
BTP Basic Transport Protocol
C-V2X Cellular-V2X
CA Certificate Authority
CAM Cooperative Awareness Message
CDMA Code Division Multiple Access
CH Cluster Head
CIA Confidentiality, Integrity and Availability
CR Cognitive Radio
CRN CR networks
CSI Channel State Information
CSMA/CA Carrier Sense Multiple Access with Collision Avoidance
DENM Decentralized Environmental Notification Message
EAP Extensible Authentication Protocol
EE Energy Efficiency
eNB evolved NodeB
ES-FDST Eavesdropping Suppression by Full-Duplex technology and Signal Transformation
ETSI European Telecommunications Standards Institute
eV2X enhanced V2X
FDD Frequency Division Duplex
FDMA Frequency Division Multiple Access
FEC Forward Error Correction
GNSS Global Navigation Satellite System
HARQ Hybrid automatic repeat request
I2V Infrastructure-to-Vehicle
IBC Identity-Based Cryptography
ICS Industrial Control Systems
IMSI International Mobile Subscriber Identity
IoV Internet of Vehicles
IRS Identity Revocation Server
ITS Intelligent Transport System
ITS station An end node in the ITS model
KMS Key Management System
LI Lawful Interception
LLC Logical Link Control
LoS Line-of-Sight
LTE Long Term Evolution

LTE-Uu Interface for communication through base station in LTE-V2X
MAC Medium Access Control
MEC Multi-access Edge Computing
MME Mobility Management Entity
mmWave millimeter wave
MNO Mobile Network Operators
NAI Network Access Identifier
NAS Non-Access-Stratum
NFV Network Function Virtualization
NIST National Institute of Standards and Technology
NOMA Non-Orthogonal Multiple Access
NR New Radio
OFDMA Orthogonal FDMA
OMA Orthogonal Multiple Access
P-SUAC Prioritized Secondary User Access Control
P2PCD Peer-to-Peer Certificate Distribution
PC5 Direct link interface in LTE-V2X
PDCP Packet Data Convergence Protocol
PHY Physical layer
PKG Private Key Generator
PLS Physical Layer Security
RLC Radio Link Control
RRC Radio Resource Control
RSU Road Side Unit
SC Superimposed Coding
SDN Software Defined Networking
SDR Software Defined Radio
SE Spectral Efficiency
SEAF Security Anchor Function
SEIES Spectral Efficiency Improvement and Eavesdropping Suppression
SIC Successive Interference Cancellation
SNR Signal-to-Nose Ratio
SUCI SUbscription Concealed Identifier
SUPI Subscriber Permanent Identifier
TDD Time Division Duplex
TDMA Time Division Multiple Access
UA-SU Unauthorized Secondary User
UE User Equipment
URLLC Ultra-Reliability and Low-Latency Communication
USIM Universal Subscriber Identity Module
V2I Vehicle-to-Infrastructure
V2V Vehicle-to-Vehicle
V2X Vehicle-to-everything
VANET Vehicular Ad-Hoc Network
VC Virtual Cell
VLC Visible Light Communication

WAVE Wireless Access in Vehicular Environments
WAVE MAC WAVE Medium Access Control
WSMP WAVE Short Message Protocol

List of Figures

List of Tables

1

Introduction

Cooperative vehicles is a topic that interests many industrial companies as well as research institutions worldwide today. The European Telecommunications Standards Institute (ETSI) has produced standards for vehicle-to-everything (V2X) communications for Intelligent Transport Systems (ITS). These standards include an overall architecture, a protocol stack and security requirements and mechanisms [45].

Meanwhile, the 3rd Generation Partnership Project (3GPP) has investigated the possibility to use the Long Term Evolution (LTE) for V2X communications [41], [42]. LTE is a cellular technology that didn't quite fulfill the ITU IMT-Advanced (4G) requirements (Release 8) but its later version called LTE-Advanced (Release 10) did. ETSI produced standards for these communications as well, including general enhancements of LTE for V2X [56], [57]. However, the ETSI ITS standards proved to be more efficient and stable compared to LTE V2X [36].

With the introduction of 5G and the New Radio (NR) technology, a huge improvement from previous generations in terms of efficiency, reliability and speed is expected to take place. The development of 5G started in 2015 and from that moment, the standards have been developed to support traditional cellular networks as well as new kinds of end nodes, such as IoT and cooperative vehicles [10]. NR will bring new technologies that enable e.g., broader bandwidth and higher speeds.

However, there is a subject that has not yet been discussed thoroughly in the literature, i.e., how 5G will affect the security of V2X communications. The new NR technologies might also bring new security challenges. On the other hand, 5G might bring new security possibilities and render some of the security mechanisms in the current ITS model redundant.

This thesis is part of a bigger project at Chalmers. The project complements the ongoing research on 5G communications within the EU 5G Infrastructure Public Private Partnership (5G-PPP), namely the mmMAGIC [7], the 5GCAR [8] and the ChaseOn Mantua [5] projects. It is also related to other V2X projects at Chalmers and the Vinnova/FFI projects Holisec [6] and BAuD [4], where Chalmers, Volvo AB and Volvo Car Corporation focus on enhancing security and privacy in the next generation of vehicles. One of the main goals of the project is to combine researchers, who have knowledge in 5G communications, with others, who specialize on security of the higher layers of the ITS stack.

1.1 Aim of the thesis

The purpose of this thesis is to investigate how 5G will affect the current V2X communications standards defined by ETSI. Both security improvements and new vulnerabilities that 5G NR brings are analyzed. Also possible reductions are discussed of the security mechanisms that the standards currently define explicitly higher up in the protocol stack.

1.2 Motivation and research questions

Currently the link-layer protocol used in V2X communications is 802.11p, which has many limitations such as speed and offers no security. With the active development of 5G, many companies and research institutes are now interested in using the new technology in V2X communications. Some features of 5G NR that differ greatly from 802.11p introduce new possibilities, as well as potential vulnerabilities, in link-layer security. More specifically, the security mechanisms that are now implemented explicitly higher up in the ETSI ITS stack, might be replaced by functionality provided at the link-layer by 5G and thus might be redundant. On the other hand, some of the new features might introduce new privacy issues, which are described in this report.
The five main questions that this thesis aims to answer are the following:

- RQ1: What protocols and security mechanisms have been used this far in ETSI V2X communications?
- RQ2: What are the security requirements for the different ETSI ITS use cases?
- RQ3: Which features of 5G NR can be used to improve security at the physical layer? Could some security mechanisms be simplified or entirely removed from higher layer protocols?
- RQ4: What new vulnerabilities could 5G NR bring to the V2X communication?
- RQ5: Is it possible to exchange 802.11p with 5G NR with no or minimal changes to the higher layer protocols? If not, what are the obstacles?

1.3 Scope

Due to time and resource restrictions, the thesis is limited to a certain scope. Some of the limitations are the following:

- This is a general study, which means that it does not analyze the details of implementation of each protocol and the corresponding message structure. Only the security mechanisms of the protocol stack and other relevant knowledge for the general understanding are covered.
- Abstractions are made from the implementation of the link-layer protocols (802.11p and 5G NR). The thesis only includes the necessary information to compare these and find the differences (primarily in terms of security).
- Due to time restrictions, a physical implementation of the new protocol stack, i.e., 5G integrated into the ITS stack, is not included.

- The thesis does not aim at solving all problems in exchanging 802.11p with 5G. The goal is instead to investigate if the exchange can be done easily and if not, present the detected obstacles.
- Lastly, the thesis does not aim at finding all possible optimizations of the security mechanisms for the new protocol stack. Rather, the gathered information is analyzed with the goal to localize several possible optimizations.

1.4 Methodology

In order to solve the research questions, a thorough study of existing technologies is first performed. These include the current ETSI ITS protocol stack for connected vehicles, the ETSI security standards and the current state of 5G. Most of the papers studied were found through IEEE Explore and through the references given in the papers found on IEEE Explore. Since there are so many academics and industrial experts involved in the bigger project, some of them were interviewed to gain a deeper insight in the state-of-the-art systems and the current state of the research. On the basis of the gained knowledge, the security requirements for the different ITS use cases were analyzed. The thesis further includes a search for possible minimizations of the security mechanisms higher up in the ETSI ITS stack. Due to new link-layer features provided by 5G, some of the higher layer security mechanisms are now redundant and could be either reduced or removed completely.
Finally, we evaluate whether the switch from 802.11p to 5G NR can be easily performed and the possible obstacles are analyzed. Due to the novelty of 5G NR, 802.11p is instead compared to the already standardized LTE V2X, which is also a cellular technology. The crucial differences between the two protocols are identified.

1.5 Overview

The rest of this report is structured as follows. First, the study of existing literature on the subject is described in chapter 2. The research is divided into several topics for the reader's convenience: the security mechanisms provided by ETSI ITS, 5G security, 5G versus 802.11p and 5G in V2X communications. After that, the knowledge provided by the literature is analyzed in chapter 3, to answer the research questions of this thesis. Finally the results are discussed and summarized in chapter 4 and concluded in chapter 5.

2
Literature study

In order to answer the research questions of this thesis, a literature study of the state-of-the-art technologies was performed. The fields of interest are the ETSI ITS and the IEEE WAVE standards, 5G, cellular V2X and 5G NR. In all of these fields, security was studied thoroughly. This chapter summarizes the main findings of the literature study.

2.1 The ETSI ITS standard

ETSI has provided several standards for the ITS Communication (ITSC). These include the communication architecture [46], the protocol stack [48], [51], the messages [44], [47] as well as the security requirements [50], services and architecture [45], [49], [52]. In these standards, the end nodes are called ITS stations. The standards are summarized in [70], which also presents an implementation and a vulnerability assessment. In the following Subsections, the architecture and protocols are described, followed by the security mechanisms and finally the Basic Set of Applications (BSA) defined by ETSI.

2.1.1 Communications architecture and protocols

The communications architecture, along with the most important protocols in each layer of the stack, are presented in Figure 2.1. The application layer consists of a Basic Set of Applications (BSA). The applications request the services in the facilities layer to encode messages, such as Cooperative Awareness Messages (CAM) and Decentralized Environmental Notification Messages (DENM). These messages are then sent to the Basic Transport Protocol (BTP) that provides a connectionless end-to-end transport service. After that, the packet is sent further down to the GeoNetworking protocol that is responsible for routing the packet through the network, from source to destination. Finally, the 802.11p protocol is used for the wireless transmission of the packet in a frame. At the destination, the message is then unpacked in the opposite direction through the stack.

The Management layer is responsible for managing the whole communication, such as cross-layer management and congestion control, as well as maintaining information about neighboring nodes. The Security layer includes all the security mechanisms of the communication and is the main focus of this thesis.

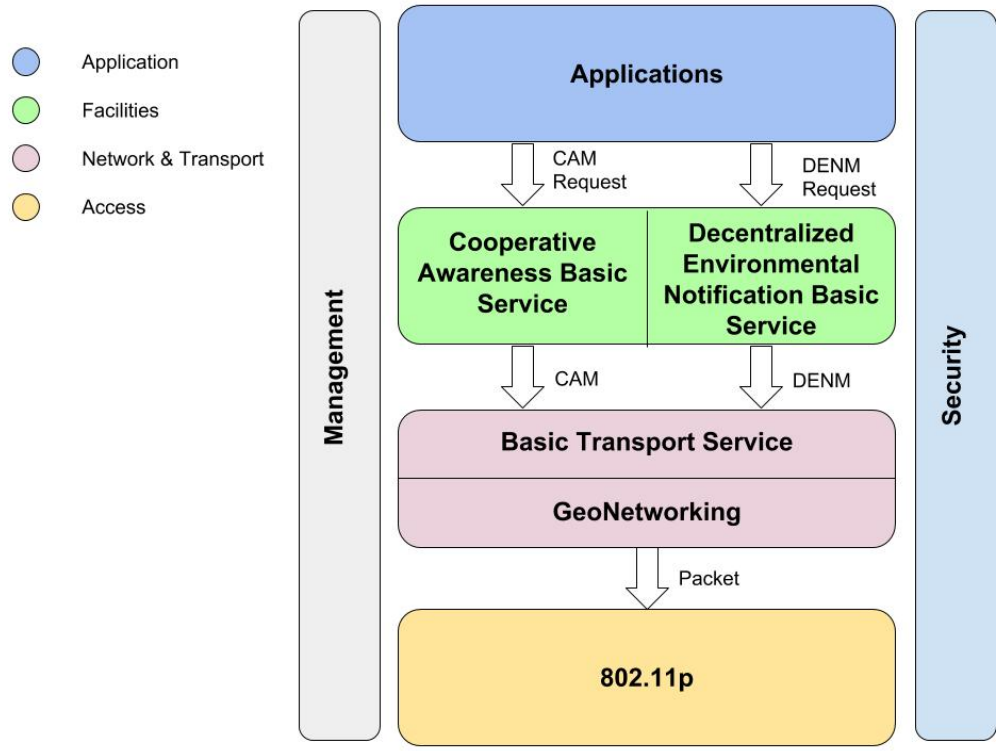


Figure 2.1: The ETSI communications architecture and protocol stack. The colored blocks represent the layers, while the arrows show the messages between layers.

2.1.2 Security

The security provided by the ETSI ITSC is summarized in a table in [45], where the services are divided into the three CIA categories: Confidentiality, Integrity and Availability. The two main components of the ETSI ITS security are the SecuredMessage and the certificate structures.
The SecuredMessage structure consists of the payloads, e.g., CAM or DENM, and the different security headers and trailers required for the Security layer. The entire SecuredMessage is then extended by each of the headers of the protocols in the lower layers of the stack. The format of a SecuredMessage for a DENM message is shown in Figure 2.2. Each of the security headers should include the length of the header (at the very beginning) as well as the type of the next header. This applies also to the payload, which should also include the length of each payload individually. The security trailer should specify the next trailer type. The SecuredMessage begins with a protocol version. It is followed by the security profile, which is used for the encoding and decoding of the message and specifies the message format as well as mandatory header, payload and trailer fields.
The certificate structure provides identification and authorizes the user to perform certain operations in a given geographical area. Different certificates are issued by different Certificate Authorities (CAs) that are structured in a hierarchy, consisting of a Root CA, an Enrollment CA and an Authorization CA (see Figure 2.3).

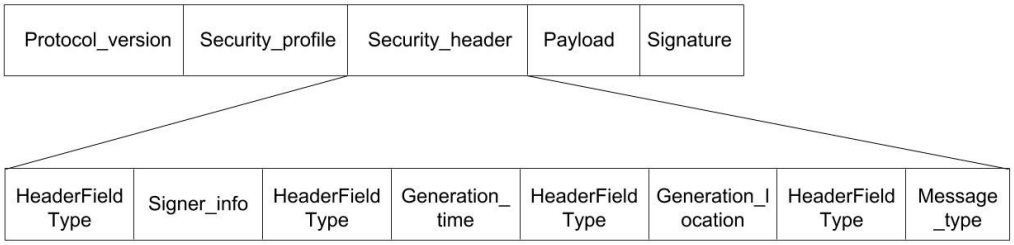


Figure 2.2: The SecuredMessage format for a signed DENM

The Root CA is the "ultimate root of trust" [50] in that hierarchy. In order to authenticate a message, the receiver needs to have access to at least the Root Certificate. The Enrollment CA uses the canonical identity (provided to the vehicle by the manufacturer) and produces a long term certificate proving the ITS station's identity. It contains a pseudonym, i.e., a temporary name, for the ITS station that should be updated regularly. The certificate is signed by the CA. This certificate is then used to prove the identity of the ITS station to an Authorization CA. The Authorization CA then produces certificates that give the ITS station permission to perform certain requested operations.

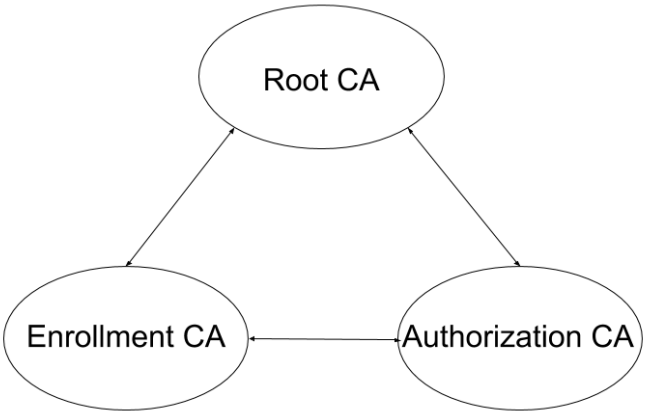


Figure 2.3: The hierarchy of certificate authorities

As shown in Section 3.2, Since most messages such as CAM and DENM are broadcasted to everyone whom it may concern, there is no need to encrypt these messages. The messages passed between the ITS station and the CAs are encrypted using asymmetric keys. Integrity and authentication is provided by the use of cryptographic signatures. The previously mentioned use of pseudonyms also provides privacy of the ITS station, since the pseudonym cannot be linked to the canonical identity of the ITS station. It is also for privacy reasons that the pseudonym should be updated regularly.

2.1.3 Basic Set of Applications

The ETSI ITS standard includes a Basic Set of Applications (BSA) [43], that describes different message types that are required for different use cases. There are around 30 such use cases. These are divided by application, where several applications form an application class. A summary is shown in Table 2.1.
The biggest application class is **Active Road Safety** and includes the two applications **Co-operative Awareness** and **Road Hazard Warning**.
Co-operative Awareness use cases focus on informing the surrounding vehicles of some special behavior of the car, i.e., *slow vehicle indication*, *intersection collision warning*, *overtaking vehicle warning*, *lane change assistance* and *co-operative glare reduction*. It also includes use cases where the special behavior is due to the vehicle being of a special kind, e.g., the *emergency vehicle warning* and the *motorcycle approaching indication*.
The **Road Hazard Warning** includes messages that are only sent when there is a sudden hazard risk in the traffic. Such cases are the *emergency electronic brake lights*, *wrong way driving warning*, *traffic condition warning* (e.g., traffic jam), *signal violation warning*, *roadwork warning*, *pre-crash sensing warning* and *collision risk warning*. The last one includes collision risk with pedestrian, with another vehicle and collision risk of two road users detected by a Road Side Unit (RSU). There are also a couple of warnings for *stationary vehicle* (accident or vehicle problem). Finally, the **Hazard Risk Warning** application includes a special group of use cases, called the *decentralized floating car data*. In these use cases, the warning message is repeated from one vehicle to another, in order to better spread the warning to vehicles approaching the place. The warnings include *hazardous location* (e.g., pothole), *precipitations*, *road adhesion* (e.g., slippery road), *visibility* and *wind*.
There are also three smaller application classes, i.e., **Cooperative traffic efficiency**, **Co-operative local services** and **Global internet services**.
The **Cooperative traffic efficiency** group is aimed at optimizing the traffic efficiency by using Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communications. This group consists of the **Speed management** application and the **Co-operative navigation** application, i.e., traffic information, route guidance, limited access warning and detour notification and in-vehicle signage. Most of these messages are issued by RSUs, but there are a couple of exceptions, such as the *co-operative adaptive cruise control* and the *co-operative vehicle-highway automation system* (platoon).
The **Co-operative local services** group consists of the **Location based services** application and aims at enabling RSUs to deliver local services to passing vehicles. Some use cases are the *point of interest notification* (shopping centers, parking lots, etc.), *automatic access control and parking management*, *ITS local electronic commerce* and *media downloading*. The *automatic access control/parking access* use case enables an RSU in control of a parking lot to automatically identify an authorized vehicle and allow it to enter. The *ITS local electronic commerce* allows an RSU to inform vehicles that a *point Of interest* can process a local payment (using some electronic purse/wallet). All of the **Location based services** are issued by an RSU to the vehicles in its surrounding.
Global internet services allow vehicles and RSUs to connect to the global net-

Applications Class	Application	Use case
Active road safety	Driving assistance - Cooperative awareness	Emergency vehicle w.
		Slow vehicle indication
		Intersection collision w.
		Motorcycle approaching ind.
		Overtaking vehicle w.
		Lane change
		Glare reduction
	Driving assistance - Road Hazard Warning	Emergency electronic brake lights
		Wrong way driving w.
		Stationary vehicle
		Traffic condition w.
		Signal violation w.
		Roadwork w.
		Collision risk w.
		Dec. floating car data
		Collision unavoidable
Cooperative traffic efficiency	Speed management	
	Cooperative navigation	
	Other	Platoon
		Adaptative cruise control
Cooperative local services	Location based services	Point of Interest notification
		Automatic access control/ parking management
		local electronic commerce
		Media downloading
Global internet services	Communities services	Insurance/financial services
		Fleet management
		Loading zone management
	ITS-S life cycle management	Vehicle software/data provisioning and update
		Vehicle-RSU data calibration
	Other	Instant messaging
		Personal data synch.
		stolen vehicle alert
		Remote diagnosis

Table 2.1: Summary of the ETSI ITS Basic Set of Applications

work. The two applications **Communities services** and **ITS station life cycle management** include such use cases as *insurance and financial services*, *fleet management*, *loading zone management*, *vehicle software/data provisioning* and *vehicle and RSU data calibration*. *loading zone management* enables a smart time allocation for freight deliver vehicles to access a loading zone. The *vehicle and RSU data calibration* enables RSUs to compare their sensor data to the sensor data of passing vehicles. Vehicles can also calibrate their sensors through V2V. The **Global internet services** application class also includes use cases for *instant messaging*, *personal data synchronization*, *stolen vehicle alert* and *remote diagnostics*.

2.2 The IEEE WAVE standard

IEEE has introduced a similar standard for V2X communications, namely the Wireless Access in Vehicular Environments (WAVE) standard [64] that is used primarily in the US. As this thesis focuses on the ETSI standards, WAVE is only discussed briefly to demonstrate that there are multiple standards for V2X communications. WAVE is similar to the European standard, in terms of both architecture and security mechanisms. Figure 2.4 shows the WAVE stack, where the colors are used to demonstrate which the corresponding ETSI ITS layers are. The main difference in the stack can be found in the higher layers, where UDP/IP or the WAVE Short Message Protocol (WSMP) is used instead of BTP/GeoNetworking in the ETSI ITS standards. WSMP is a protocol for rapid exchange of messages that minimizes communications overhead. The WAVE Medium Access Control (WAVE MAC) and the physical link (PHY) are both part of the 802.11p standard used in ETSI ITS. The Logical Link Control (LLC) wraps and unwraps the packet to be passed on to different lower and higher layer protocols respectively [63]. In WAVE, the protocols and services above UDP and WSMP are not specified.
The security services of WAVE support traditional cryptographic mechanisms, e.g., symmetric/public keys for encryption/signing, hashing and certificates provided and verified by an authority infrastructure. Certificates can be either explicit (includes the public key explicitly) or implicit (includes a reconstruction value for the public key). Further, the standard supports peer-to-peer certificate distribution (P2PCD). This is used when a vehicle receives a signed message for which the WAVE Security Services cannot construct a certificate chain. The reason could be that it cannot recognize the issuer of the topmost certificate in the message.
Privacy mechanisms are mentioned very briefly. The only privacy mechanism specified is a periodical change of certificate.

2.3 5G architecture and security

The new generation of cellular networks, 5G, emerged recently as a research topic and is now one of the leading subjects in the technical field around the world. Many papers have been written about it during these last three years. This Section first presents an overview of the security of 5G in general and then zooms in on the physical layer security issues and solutions.

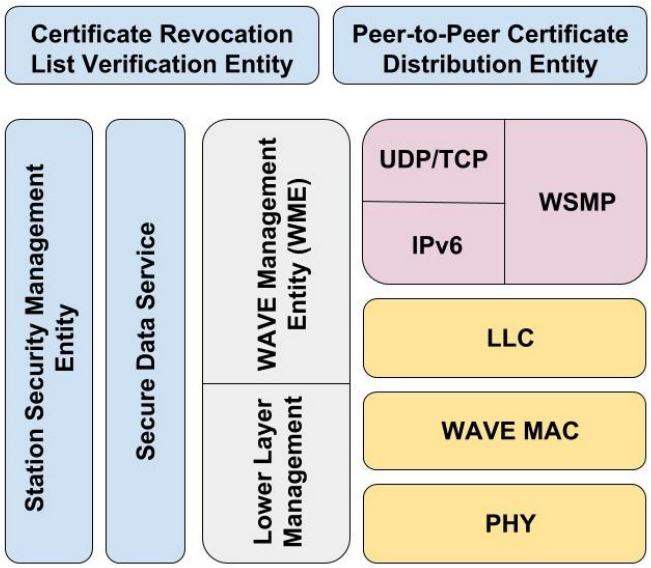


Figure 2.4: The IEEE WAVE standard protocol stack.

2.3.1 An overview of 5G security

There are many papers that give an overview of the state-of-the-art security of 5G, such as [14], [34], [18] and [90]. Institutions that are interested in 5G have also published whitepapers on this matter, such as the Ericsson whitepapers [33], [12] and several papers by Huawei [39], [40]. Even if these papers do not directly answer the research questions of this thesis, they were still included in the literature study to give an overview of the ongoing research around 5G.

A broader security analysis is given by Ahmad et al. [14], where the authors describe the security threats in 5G networks and possible solutions from mostly the software level. The challenges of the newly introduced Software Defined Networking (SDN) and Network Function Virtualization (NFV) concepts are discussed. SDN separates the network control plane from the data forwarding plane in order to enable network function softwarization. NFV enables moving functionality from one network unit to another just by changing the software. Thus, it eliminates the complexity of changing a network with specialized hardware. Also new privacy threats are presented, such as false base stations that get hold of the International Mobile Subscriber Identity (IMSI) of users. IMSI is used to authenticate users to connect to the network. Finally, different solutions for these issues are mentioned briefly, with references to other papers that are described in this report as well.

The challenges of using the SDN and NFV concepts for virtualization are also discussed by Arfaoui et al. [18]. Network slicing is described as a technology that divides the network into smaller logical dedicated networks. These are "composed of virtualized and non-virtualized resources that can be instantiated and customized to fulfill a set of requirements". Challenges introduced by network slicing are also presented in the paper. One of these is the fault propagation effect, that is the result of

a fault at the physical layer that propagates to overlying virtual resources. Another problem is the cascade effect, when an attack propagates between the slices through shared resources or communication channels. Privacy threats are divided according to the target: user identifier and user data. As opposed to user privacy, authorities should be able to wiretap suspicious users and for this Lawful Interception (LI) should be used. Finally, in the related work the authors refer to the 5G-ENSURE project.

The 5G-ENSURE project [1] is funded by the EU Framework Programme for Research and Innovation H2020 and drives the 5G security vision for the European 5G-PPP. Among its achievements are contribution to the 5G architecture described by 5G-PPP [37] and a test-bed that was launched at the b<>com campus in Rennes in 2016 [3]. The project also has 41 contributions that were presented to ETSI and the security group 3GPP SA3 and a regular interaction with the US National Institute of Standards and Technology (NIST).

The paper by Zhang et al. [90] gives an overview of the work progress of the System Architecture group 3GPP SA2 and the Security group 3GPP SA3 that will provide specifications for 5G. New concepts such as network slicing and allowed non-3GPP access (i.e., that other link layer technologies are allowed) are introduced and the architecture of 5G is presented. The new security architecture is described as well, with several new entities such as the Security Anchor Function (SEAF), which creates a unified anchor key for the primary authentication. The security anchor key created by SEAF would then be used to derive the Access Network key and the Non Access Stratum (NAS) keys. NAS is defined as "the signaling protocol of the UE for mobility and session related control messages". User data is secured in terms of confidentiality and integrity by also using cryptographic keys.

As the paper [90] describes, authentication consists of two stages: primary and secondary authentication. The primary authentication provides access to the 5G core, while the secondary is used between an enterprise and user equipment (UE) to provide access to, e.g., a corporate APN (a gateway between a mobile network and the Internet). The new version of IMSI, which is called the Subscriber Permanent Identifier (SUPI), will be protected through public key encryption instead of being sent in cleartext. The Universal Subscriber Identity Module (USIM) is the successor of the SIM application in traditional SIM-cards. Protection mechanisms in the UE USIM are defined as well as secure network slicing. The paper also presents two use cases for 5G, i.e., V2X communications and IoT. In the case of V2X, the authors refer to ETSI documents that will be discussed further on in this report (see Subsection 2.4.2).

In one of its whitepapers, Ericsson states that the IMSI is not yet protected, because the cost to do this has until now out-weighted the benefits [33]. The whitepaper also mentions a 5G for Sweden research program as well as 5G-ENSURE that was discussed earlier. Network slicing is proposed for isolation and secure ID management. To secure these, it is proposed to create a baseline unified security standard for all slices and additionally application specific security for the different slices. Identity management should use the USIM technology as in 4G LTE (advanced LTE), but also allow enterprises with good existing ID management mechanisms to use these in their 5G connection. LTE radio access has good protection against eavesdropping

but not against modification or data injection, which are new security concerns in cellular networks [33]. Other such concerns are protection against DoS, light-weight encryption solutions for power sensitive entities (IoT), cloud security and new trust models that handle misbehaving entities.
The Huawei Technologies Co. whitepapers mostly agree with the ones by Ericsson [39], [40], i.e., network slices are also proposed for virtual isolation. Additionally, in [39] it is stated that hop-by-hop network security is not enough. There is thus a need for end-to-end security to reduce the reliance on the cloud, for flexible data protection for different services and to eliminate hop-by-hop encryption and decryption [40]. Standardized security assessment metrics should be agreed upon, to simplify the transition between different access technologies. A unified authentication framework, such as the extensible authentication protocol (EAP) framework, could be implemented for this. At the same time, security policies should be flexible.
Authentication and privacy are two main issues that need to be improved [39]. A new idea presented is that the telecom operators could provide their advanced security mechanisms as a service to users and vertical industries. Many new connected devices, such as sensors, are either too small or too cheap to have a USIM, so new identity management technologies are needed [39]. Identity-Based Cryptography (IBC) is introduced, where there is no need for certificates, since the technology uses the device ID as a public key. This reduces message length and delay and is thus a good solution for the Internet of Vehicles (IoV) [40]. IBC is explained further in Subsection 2.4.5.
A solution for user privacy is using random IDs instead of transmitting permanent IDs over air. However, even if not transmitted, the IMSI should be protected and the protection should be compatible with LTE station authentication. For confidentiality of IoT devices, it is proposed to use asymmetric cryptography, but there is a need for more efficient algorithms [40].
Another new security concern is that the new IT technologies (e.g., SDN and NFV) [39] as well as IoT [40] might increase DDoS attacks. A countermeasure is to use decentralized authentication. This implies no single-point-of-failure, as in the case with centralized authentication servers. It also allows shortening distances, i.e., the server can be moved to the edge of the network, which would also benefit the asymmetric key management system. End-to-end user plane protection goes between the UE and egress gateways on the operators' networks. Thus, also the egress gateways can be moved from the central core to the edge to minimize transmission distances. [40]

2.3.2 Recent advances

The most recent whitepaper published by Ericsson on 5G security (at the time of writing this thesis) [12] gives a high-level overview of the different technologies to be used in 5G in this field. It lists five features that ensure trustworthiness: resilience, communication security, identity management, privacy and security assurance.
For resilience, a separation and isolation approach is used, e.g., network slicing and dividing each base station into two units: one central and one distributed. When it comes to communication security, both signaling and user plane traffic is

encrypted. Further, signaling traffic is integrity protected and this option is available for the user plane traffic as well. The identity management provides partly the same mechanisms as for 4G, i.e., secure cryptographic functions and keys and mutual authentication between the network and end user. Further, it also describes the EAP framework. This framework provides more flexibility for the mobile operators to choose parameter formats for authentication. Also the 5G authentication and key agreement (5G-AKA) mechanism is used for authentication and session key distribution [19]. The session keys cryptographic symmetric keys and AKA is based on challenge-response mechanisms. AKA is also used in the 3rd generation mobile networks, for both IP multimedia service and radio network authentication purposes. The user (devices) identities and formats used are the IMSI for the radio network and the Network Access Identifier (NAI) for the IP multimedia service uses. Privacy is provided by encryption of identifier, a protection mechanism for the long term identifier and regular refresh of the temporary identifier. The security assurance is used to ensure that network equipment meets security requirements and in this certain case, it consists of security requirements and an auditing infrastructure.

Quite recently, the University of Oxford published a technical report showing a vulnerability of the currently proposed version of the 5G-AKA protocol [28]. The report first describes the 5G-AKA protocol, which is based on the previous version used in LTE/4G. The four entities involved in the authentication are the UE, the Security Anchor Function (SEAF), the Authentication Server Function (AUSF) and the Authentication credential Repository and Processing Function (ARPF). The last three entities are considered within the 5G Core Network and the last two are within the Home Network. The UE and the SEAF can be remote or roaming.

When running the AKA protocol, the UE authenticates using the SUbscription Concealed Identifier (SUCI) instead of the SUPI, which should never be revealed publicly. The user device's long-term secret symmetric key, K, is only known to the UE itself and the ARPF. The result of the protocol is an "anchor key" K_{SEAF}, that is further used the derive session keys for communication between the UE and the SEAF.

The attack exploits a race-condition, where an attacker (B) initiates two sessions at about the same time. In the first session, an overheard SUCI (of user A) is used. In the other, B's own USIM and SUCI are used. Because of this race condition, the AUSF will not be able to distinguish between the two responses from the ARPF. This may lead it to associate the wrong response (and the resulting keys) with the wrong user. As a result, B can derive the anchor key, which can be used to impersonate user A to the network.

The report also proposes a couple of easy solutions. The first one is to include the SUCI in the responses from the ARPF. In that way, the responses will be differentiated and matched to the corresponding request. The other solution is similar and involves a tighter binding between the request and the response. This can be done in several ways, e.g., by including a fresh (unique, random) value in both the request and response or by establishing a TLS session between the AUSF and the ARPF.

2.3.3 Wireless physical layer security in 5G

Among the research papers discussing 5G security, there are those that focus on the security of the physical layer. The two main areas are physical layer security (PLS) and physical layer authentication.

In their paper, the authors Sun and Du [78] explain how PLS can be used in different 5G use cases for confidentiality. PLS technologies using artificial noise injection are presented, i.e., when noise is introduced to degrade the channel quality of the eavesdropper while the receiver's channel quality stays high. Other technologies for modifying the signal to avoid eavesdropping are also presented. It is motivated that PLS is faster than cryptographic approaches and removes the need for key distribution. Also, PLS provides multiple security levels, unlike cryptographic solutions. Given the new features of 5G networks (such as their different QoS requirements and limited power, storage and processing capabilities of the IoT devices connected) the current PLS technologies are not completely suitable for 5G.

The paper [78] instead proposes several new PLS solutions for meeting the new requirements of 5G. For the scenarios that require ultra-low latency, like vehicular networks, a fast PLS solution is proposed. It is based on the idea that an eavesdropper should not be able to accumulate a given amount of data during a certain period, to be able to decipher the sender's information.

Physical layer security has also been targeted by Farhang et al. [35], where the authors explain a privacy vulnerability due to the new physical features provided by 5G NR (see Figure 2.5). Since the cells of access points are smaller, the preference of a mobile user can reveal its location. For users in the intersection of two access point cells, the location could be determined even more precisely. The authors also propose a solution using a differentially private mechanism that introduces "noise" to the choice of access point. The same problem is addressed in [89], where Yu et al. propose a different solution using distributed knowledge. This solution requires an infrastructure consisting of several additional entities, unlike the solution in [35]. At the same time, they mention a few other papers with more ad-hoc solutions, i.e., without a trusted third party.

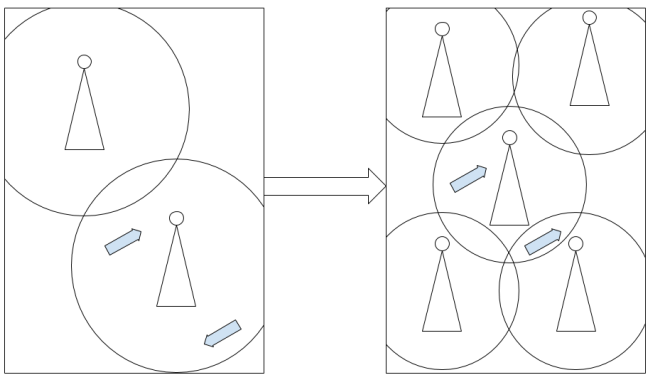


Figure 2.5: In 5G, there will be more base stations with smaller cells. The arrows symbolize connected vehicles.

Sun and Du [78] also target physical layer security for 5G networks. In this paper, the authors present several different use cases where PLS provides confidentiality. One of these use cases is securing vehicular networks. Due to the restriction of a low delay tolerance, the traditional PLS technologies are inefficient in this concept. Instead, a so called statistical security model is proposed, which builds on the probability that an eavesdropper cannot collect a certain amount of data (a threshold) needed to extract useful information.
The authors Pan et al. [72] present physical layer authentication. This kind of authentication is based on the channel response, which is unique for a specific sender at a specific location. The channel response is used as a fingerprint due to these unique features. A prior channel response is saved and then compared to future channel responses to confirm that they correspond to the same transmitter. It does not add any additional cost, since it takes advantage of channel estimation, and it takes less than 1/100 of the time the upper layer authentication takes. In their solution, the authors use higher layer cryptography-based authentication to initially authenticate the users. The channel response is then used for re-authentication.
The channel response has also been used by Xie et al. [84] in a key distribution process, to authenticate the sender of a symmetric key. They also make measurements which prove that the channel response is unique for a certain sender and location. Thus, it is reliable to be used for authentication.

2.4 5G in V2X communications

The definition of 5G is expected to cover many more applications than just mobile phone communication. One of these fields, that is the focus of this thesis, is V2X communications. 5G-PPP has also started a Phase-2 project called 5GCAR in June 2017, that has a duration time of 24 months [8]. The goal of the project is to investigate how 5G can be adapted to be used in V2X [27]. Approximately 30 persons are working full time on this project and the consortium consists of institutes and companies such as Chalmers University of Technology, Huawei, Ericsson, Volvo Group, Nokia and Bosch.
This Section first presents the evolution of cellular V2X, followed by ETSI standards for 5G in V2X communications. Further, it discusses research papers in this field and more specifically about the security of these communications, both overall and on the physical layer. Finally, papers comparing cellular V2X to 802.11p are presented.

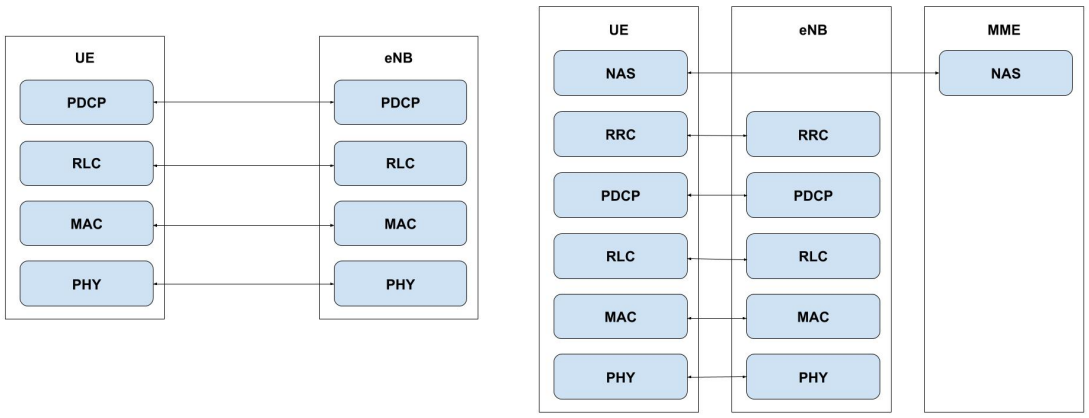
2.4.1 The evolution of cellular V2X

The first models for cellular connections in V2X were developed for LTE, called cellular V2X C-V2X. Initially, C-V2X only allowed vehicles to communicate through the cellular infrastructure. The connection included a V2I uplink to the infrastructure and a I2V downlink to the receiving car [80]. This type of connection is time consuming and not suited for the ad-hoc solutions required for V2X. Also, the centralized structure creates bottlenecks and single-point-of-failure at the base stations [80].

Thus, a new version of LTE was created, namely LTE A-Pro (Release 14). The requirements for this can be found in TS 122 185 [56] and the LTE architecture enhancements for V2X in TS 123 285 [57], and are further presented in the next Section (2.4.2). The architecture includes the PC5 interface for direct V2V communication (also called sidelink) [60], [80] (see Figure 2.6). The traditional communication through base stations goes through the LTE-Uu interface. Messages sent over the LTE-Uu interface are wrapped in UDP/IP packets and the PC5 interface supports both IP based and non-IP based messages. The technology is basically the same as in the ETSI ITS standard, but is less mature than this well-established technology using 802.11p.

Figure 2.6: A demonstration of the V2V communication (sidelink) through the PC5 interface

The latest frozen version of cellular communications for V2X is 5G V2X (called eV2X) Release 15, with Release 16 still under development. One of the main ideas of eV2X is to combine all the previous technologies, such as ETSI ITS and cellular V2X. A vehicle should be allowed to use any of the technologies available at the moment. This way, cellular V2I can be used when appropriate and ETSI ITS can be used for V2V whenever possible, in order to optimize speed. This is called Multi-RAT [24] and it is possible because the payloads of the LTE frame are the same as for ETSI ITS, i.e., CAM and DENM are used. However, the headers wrapping the CAM and DENM differ. In LTE, these include the user SIM for authentication as well as the ID of the currently connected base station. Also the wireless transmission technology differs.
Another new technology called Multi-access Edge Computing (MEC) is also introduced in eV2X [68]. MEC brings servers to the edge of the network and thus closer to the user, which reduces latency and increases connection speeds. Further, network slicing will be used to virtually separate different services into different containers [10]. In this way, services for safety, IoT, data, etc. will be allocated different bandwidths/channels, which will allow different QoS. The slices will be software defined and thus reprogrammable. The upcoming NR [36] will provide new available bandwidths. In order to improve throughput, there will be more base stations with a smaller capacity [35].

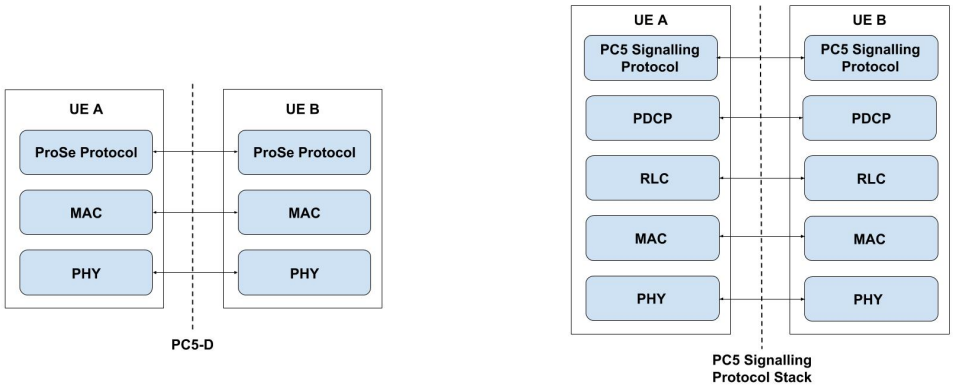


(a) The user plane protocol stack **(b)** The control plane protocol stack

Figure 2.7: The protocol stacks for communication over the LTE-Uu interface

2.4.2 ETSI standards

During the latest years ETSI started producing standards for 5G in V2X communications and the corresponding security requirements. The stack for the communication between the UE and the base station (eNB) over the LTE-Uu interface is described in TS 136 300 [55] and is presented in Figure 2.7. As shown in Figure 2.7b, the control plane adds another layer (RRC) to the user plane stack.
The Non-Access-Stratum (NAS) control protocol is terminated in the Mobility Management Entity (MME) on the network side and performs functions such as authentication and other security control. The Radio Resource Control (RRC) protocol is terminated in eNB on the network side and performs functions such as broadcast, paging, RRC connection management, mobility functions and UE measurement reporting and control. The Packet Data Convergence Protocol (PDCP) sublayer is terminated in eNB on the network side and performs functions such as ciphering and integrity protection. Also, the *type* field in the PDCP header is used to distinguish between IP, ARP and PC5 Signaling Protocol (ARP is not supported for one-to-one communication). Below PDCP we find the Radio Link Control (RLC) and Medium Access Control (MAC) sublayers. These are also terminated in eNB on the network side and perform functions such as header compression, ciphering, scheduling, Automatic Repeat Request (ARQ) and Hybrid Automatic Repeat Request (HARQ). ARQ and HARQ are used to ensure a packet is received at the destination. The physical layer (PHY) finally transmits the frame. As can be seen in TS 129 468 [61], the messages from the UE to the Application Server are encapsulated in UDP/IP packets.
The PC5 discovery and signaling protocol stacks are described in TS 123 303 [58] and can be seen in Figures 2.8a and 2.8b respectively. As shown in the Figure, the discovery protocol stack uses MAC and PHY as specified in TS 136 300 [55] and the ProSe protocol is used for handling ProSe Direct Discovery as specified in TS 124 334 [54]. For the signaling protocol stack, PDCP/RLC/MAC/PHY are specified in TS 136 300 [55] and the PC5 Signaling Protocol is used for control plane signaling over PC5.



(a) The PC5 discovery plane stack **(b)** The PC5 signaling protocol stack

Figure 2.8: The protocol stacks for communication over the PC5 interface

The 3GPP TS 33.185 [59] standard specifies the security of LTE for V2X communications. This includes the security architecture, requirements and the solutions to these requirements. The requirements state that the communication between all entities should provide authentication, integrity and confidentiality of messages. It should also be protected from replays. The UE identity should also be confidentially protected on the interface between the V2X Control Function and the UE. The privacy requirements for PC5 are specified in 3GPP TS 22.185 [56], and are as follows:

- *"Subject to regional regulatory requirements and/or operator policy for a V2X application, the data sent in the PC5 transmission should not allow UE identity to be tracked or identified by any other UE or non-V2X entity beyond a certain short time-period required by the V2X application.*
- *Subject to regional regulatory requirements and/or operator policy for a V2V/V2I application, the data sent in the PC5 transmission should not allow a single party (operator or third party) to track a UE identity in that region."*

Additionally, 3GPP TS 33.185 [59] specifies the following three requirements:

- *"The identifiers in the V2X messages should minimize the risk of leaking the UE or user permanent identities.*
- *UE pseudonymity should be provided to conceal personal data from attackers.*
- *The application layer UE identity in the V2X messages should be protected from eavesdropping."*

The provided solutions for all these requirements cannot be made mandatory for all V2X services, since each service has its own specifics. It is thus left up to the implementation of the security features to ensure that the service is properly secured. For network security, the document [59] refers to previous solutions in the TS 133 210 [42] and TS 133 310 standards [41], i.e., security solutions developed for 3G.The recipients of many of the application messages sent over V2X are not known to the sender beforehand. This implies that a network assisted security association between entities is unfeasible and current solutions such as LTE security and ProSe

one-to-many communication cannot be used [59]. Instead, the application data should be secured by the mechanisms in ETSI ITS security standards, as discussed previously in this report, or the corresponding standards by IEEE [64]. LTE-Uu communications should additionally use the LTE security mechanism for air interface confidentiality. PC5 does not provide any access layer security.
The document [59] also provides optional privacy solutions for PC5 networks, while the privacy for Uu mode communications are the same as for regular LTE (see TS 33.401 [53]). In PC5 communications, the link layer source ID and the source IP address (when IP is used) should be randomized when indicated that the application layer identifier has changed. Equivalently, the UE should inform the application when the link layer source ID and the source IP address (when used) are changed.

2.4.3 Research about 5G for V2X

There are many papers that focus on optimizing 5G for V2X communication. In the two papers by Di et al., [29], [30], the authors propose new non-orthogonal time-frequency allocation schemes to achieve low-latency and high-reliability. In their paper, Ali et al. [16] create a testbed for such high-reliability/low-latency 5G-V2X communications. Some papers focus on reducing network congestion and packet drops. Pak [71] propose a new and faster packet classification for this purpose, while Chang et al. [25] propose a new packet forwarding approach to avoid flooding and message storms introduced by broadcasts. Zhou and Kellerer [93] explore the new concept of Virtual Cells (VCs) and optimize these in terms of capacity, reliability and power efficiency. In [69], Luoto et al. instead focus on optimizing the performance of LTE communication between vehicles and RSU by letting vehicles with a better connection serve those with a worse connection to the RSU.
The paper by Chen et al. [26] provides an overview of the state-of-the-art of C-V2X and eV2X communications. The authors first describe the currently published 3GPP standards in this field (that are also discussed in this report). They state that C-V2X communications can already support certain platooning and limited automated driving applications, though much work has to be done to make it useful for fully automated driving. Further, they provide five use-case groups: platooning, advanced driving, remote driving, extended sensors and other/general. The security standards defined by the SA3 group in 3GPP are described, but security is not the main focus of the paper, unlike in [90] as described earlier in Section 2.3.1.
In their paper, Zou et al. [94] implement 5G V2X communications for fast emergency braking. The authors show that 5G could be used for V2V, as explained in [21]. This is called direct connectivity and works over the PC5 interface, as defined by the ETSI standards and explained in Section 2.4.2. The cellular connectivity utilizes the Uu interface, but is not used in the scenario analyzed by the paper. Global Navigation Satellite System based (GNSS-based) synchronization is essential in out-of-network coverage scenarios, as also mentioned in [21]. Multi-antenna provides better coverage and other important improvements to ultra-reliability and low-latency communication (URLLC) scenarios, such as the emergency brake.
During the testing phase [94], the software programs used were BISSender and BISReceiver and the utilities layer messages used were CAM, as defined by ETSI

ITS [48]. The packets are sent to Radio BBU as UDP messages and then transferred by 5G device-to-device communication. Message rates were increased to 200Hz, compared to the normal ETSI-defined 1-10Hz, because it is a time and message reception critical service. The tests show an improvement over purely sensor-based systems.

2.4.4 The security aspect of 5G in V2X

In difference to the above presented papers, Bian et al. [20] focus on the security aspects of V2X communications. They present a couple of threats not handled by the proposed standards (e.g., by 3GPP), namely the platoon disruption attack, based on replaying old control packets, and the perception data falsification attack, inserting false video frames or photos.
A cryptography-based security sub-layer is presented together with its limitations, i.e., costly computations and certain attacks (as the ones mentioned above) are not covered. Also there is no way yet to detect jamming attacks. To solve these issues, the authors propose non-cryptographic security mechanisms that could be added. An example is that a car in a platoon could first collect sensor data from other vehicles in the platoon, to see if any vehicle's sensor data deviates more than a certain threshold (called statistical interference). To avoid jamming, a channel hopping process can be established, where two communicating parties hop between channels in a sequence unknown to the attacker. Finally, the main challenge of the non-cryptographic mechanisms, according to the authors, is the time delay.
Hashem Eiza et al. [38] present a secure video reporting service in V2X networks using 5G. Their solution is similar to the ETSI standards, but instead of giving general guidelines, it explains which specific algorithms could be applied in their use case. It also balances privacy and tracing misbehaving nodes by using distributed knowledge, that is, a number of authorities have to collaborate to find the real identity of the sender of a message. In order to offload the certificate verification from the vehicles, a cloud service is used. The paper concludes with numerical results showing possible speeds of the security mechanisms over 5G. It is shown that a traffic accident can be reported to the nearest designated official vehicle within one minute, when the video size is 2GB and the cryptographic encryption algorithm used is AES/CBC. Even though providing a highly developed high-layer security scheme, the paper does not handle physical layer security.

2.4.5 Identity-Based Cryptography

The concept of IBC, which was briefly mentioned in [39] and Section 2.3.1, is a very suitable cryptographic scheme for resource-restricted devices. It has been proposed in many recent papers [73], [31], [17] for IoT devices, to efficiently encrypt and sign the exchanged messages.
The scheme was introduced as early as 1984, by Shamir [76]. The paper describes a public-key signature scheme that uses the identity of a user, along with some other known information, to produce a public key for the user. The corresponding private key is then provided by a key generation center. The center only gives each user a

smart card with the private key, along with the programs for signing/verification. When this is done, the center is no longer needed.

The paper makes the following definitions:

"- m is the message
- s,t is the signature
- i is the user‘s identity
- n is the product of two large primes
- e is a large prime which is relatively prime to phi(n)
- f is a one way function."

The values n, e and the function f are publicly known. The private key of a user is a number g such that:

$$g^e = i \ (mod \ n)$$

Using these definitions, the following algorithm is used for signing:

$$t = r^e \ (mod \ n)$$
$$s^e = g^e * r^{e*f(t,m)} \ (mod \ n)$$

Where r is a random number. Since e is relatively prime to $\Phi(n)$, it can be eliminated:

$$s = g * r^{f(t,m)} \ (mod \ n)$$

The verification of the signature is done by:

$$s^e = i * t^{f(t,m)} \ (mod \ n)$$

This scheme is secure, since breaking it would require exceedingly difficult computational tasks. The value of r should always be random and never reused.
Variants of this scheme, along with IBC encryption, have been proposed recently by many papers for securing communication in IoT and ICS networks. One of these is the paper by Peng et al. [73].
In their paper, Peng et al. present an architecture for secure publish/subscribe communication between IoT devices, wireless sensors and users. The protocol is called Another Identity-based Publish/Subscribe (AIPS) protocol and is used for encryption of data and authentication of the sender. The authors argue that this IBC-based approach is more efficient than traditional PKI, since it removes the need for certificates. Nevertheless, the algorithms for encryption are not as efficient as that of symmetric key protocols, so IBC is used to distribute symmetric session keys that are later used for encryption of data.
The architecture also includes two trust zones, the AIPS server trust zone and the application trust zone. This is done in order to separate different groups and

restrict attacks. In IBC-based protocols, the private keys are generated by a Private Key Generator (PKG) in the trust zone. For this specific system, the PKG is an administrator. In order to acquire data, an entity has to follow three main steps: address resolution, data subscription from users and data subscription from gateways. The subscription is done by using a similar IBC-based protocol.

This scheme is described by the authors as secure and at the same time a very efficient solution compared to traditional public key cryptography mechanisms. Nonetheless, they admit that any PKI protocol would not be efficient enough for very resource restricted devices.

In another paper [31], the authors Drias et al. also use IBC for key distribution (like in [73]), in this case in a Key Management System (KMS) for Industrial Control Systems (ICS). The authors mention that an identity-based encryption idea was introduced by Shamir in 1984. On the other hand, the first real functional IBC scheme was proposed by Boneh and Franklin in EuroCrypto 2001 and referred to Shamir's scheme along with other papers in the field.

Further, the two main drawbacks of IBC are discussed, i.e., key escrow and the revocation problem. Key escrow happens if the PKG has been compromised. Since it has generated the private keys for all of the system entities using its master key, it can decrypt and sign messages using these keys. In this way the PKG can violate the confidentiality and authentication properties. The revocation problem emerges when the private key of an entity has been compromised. In this case, since there is no revocation list as in traditional PKI, other users will not know that the key is no longer valid.

The paper also proposes a new scheme that solves these issues. In order to solve the key escrow problem, the authors generate the private keys for the ICS entities in an "offline" pre-operations step. When this is done, the PKG is simply not needed anymore and the key escrow problem can thus be avoided. To solve the revocation problem, the authors propose to use an Identity Revocation Server (IRS) which is a trusted entity. The IRS will contain "a database of ICS entities with the revocation status and the response validity duration. Each system entity will request its revocation status and get it time stamped and signed by the IRS. This IRS response will be used by the entities in the encryption and the signing operations." The IRS has a pair of keys (public and private) that were generated by the same PKG of the ICS.

The authors also discuss a drawback of their solution, i.e., the high computation cost due to the added exchanges between communicating entities. On the other hand, they argue that the number of exchanges is still less than in the case of PKI.

Finally, in [17] Anggorojati and Prasad also propose a scheme for securing IoT with identity-based cryptography. In the paper, a variant of IBC proposed by Zhaohui Cheng et al. in 2004 is implemented. This scheme is also free from key escrow, as the scheme in [31]. Also in this solution, much like in [73], IBC is used to distribute symmetric keys because these are more efficient.

2.4.6 C-V2X vs 802.11p

One of the research questions of this thesis was whether the switch from 802.11p to 5G NR can be made easily. In order to answer this, the two technologies should be compared to find the differences. Since 5G NR and eV2X is still under development, it is hard to compare it to 802.11p. For this reason, this chapter discusses the differences between 802.11p and C-V2X, i.e., the predecessor of eV2X. There has been a lot of research going on where the two technologies have been compared. To begin with, Table 2.2 shows a comparison between the basic features of the two technologies. As can be seen, they result in very similar speeds and bandwidths. So what are the main differences then?

LTE-V2X	802.11p
Peak downlink speeds (Mbps): 2, 50, 100 Peak uplink speeds (Mbps): 2, 25, 50	The allowed range is 1.0 to 63.5 Mbps (US) data rates
Channel bandwidths (MHz): 1.4, 3, 5, 10, 15, 20	Channels of 10 MHz bandwidth in the 5.9 GHz band (5.850-5.925 GHz)
Access schemes: OFDMA (Downlink), SC-FDMA (Uplink)	Access method: carrier sense multiple access with collision avoidance (CSMA/CA)
Modulation types supported: QPSK, 16QAM, 64QAM	BPSK, QPSK, 16-QAM and 64-QAM
error correction: CRC, HARQ (Hybrid automatic repeat request, ARQ error control + high-rate forward error correcting coding)	CRC, Forward error correction (FEC) coding
Half-duplex, FDD (frequency division duplex) and TDD (time division duplex)	Half-duplex

Table 2.2: Comparison of the basic features of C-V2X and 802.11p

In summary, C-V2X was initially developed for V2I/I2V communication and only the latest version, as described in Section 2.4.1, has an interface for direct communication, i.e., V2V. 802.11p, on the other hand, was developed primarily for ad-hoc mode, where vehicles can easily connect and communicate directly. This is done by eliminating the need to join a Basic Service Set (BSS) before establishing a connection [62]. However, this implies that there is no security in 802.11p and it completely relies on the security mechanisms of higher layer protocols. On the other hand, it can be argued that 802.11p is older and more well-established than C-V2X [36]. The papers described further will compare the two technologies more in detail.
In 2015, the 5G-PPP Group published a paper on 5G for V2X [80]. In this paper, they presented, among other aspects, the benefits and limitations of earlier physical layer technologies for V2X, namely the IEEE 802.11p protocol and LTE, a predecessor for 5G.

A benefit of 802.11p is that it is available in no-coverage areas, due to direct communication between the source and the destination. It is a WiFi protocol optimized on efficiency and speed, but is still less efficient than LTE technologies when the loads increase, i.e., in urban areas. There is also a high probability for collisions due to no scheduling infrastructure as in LTE (instead CSMA/CA is used). Also, 802.11p has a resource allocation that is not as flexible as the one of LTE and it has a shorter coverage (only several 100 meters).

In terms of security, 802.11p is the underlying protocol in the ETSI ITS stack, where security is provided through cryptographic signatures and certificates [80]. This is very time consuming and requires the introduction of a separate infrastructure. When this 5G-PPP paper [80] was written, LTE ProSe was still under development. Thus, LTE had drawbacks such as only in-coverage communication, i.e., no direct V2V. Further, the authors explain that LTE and ProSe were originally developed for other use cases and now have to be adapted to the automotive case. This includes optimizations to transmit small amounts of data as well as the security mechanisms.

In their paper, Filippi et al. [36] claim that the C-V2X is not yet ready to replace the IEEE 802.11p protocol in vehicular networks. They motivate that C-V2X is not suitable for ad-hoc networks because it requires strict synchronization and thus has a limited performance. Also they point out that C-V2X, unlike 802.11p, is vulnerable to the Doppler effect, which limits its speed. Another issue is the near-far problem: when two messages that arrive simultaneously (e.g., msg1 of high priority has a weak signal and msg2 of low priority has a strong signal) the receiver might have difficulty detecting the weak message. This can lead to important safety messages being lost. The authors also mention that there are solutions for this problem under development [36].

802.11p is shown to have a more efficient resource allocation scheme for variable payload size. Because of the half-duplex mode used by C-V2X, it has a higher latency and is less efficient than 802.11p. The authors also claim that C-V2X is bad at handling collisions, because it is not using a carrier sensing technology like 802.11p. When it comes to cybersecurity, the solutions for C-V2X will be more complex and thus more expensive.

Even though the authors argue against C-V2X, they mention the upcoming 5G that could be able to satisfy the requirements for safe and efficient V2X. However, they claim that this technology will not be ready to use for years to come and thus 802.11p is currently the leading alternative for vehicular networks.

In a recent report [11], 5G Automotive Association present a comparison of the C-V2X (PC5) and 802.11p physical layer technologies for road safety. The analysis includes reliability of the two technologies to deliver safety critical messages and the number of accidents that can be avoided in both cases. The results show that C-V2V at its current stage outperforms 802.11p in the given scenarios. Because of this, the authors argue that C-V2X should not be disregarded by EU regulations and they should not "...hinder the deployment of C-V2X (PC5) in favour of 802.11p...". The report presents the parameters used for the measurement, but does not explain why C-V2X proved to be better.

There are also a few very recent papers comparing 5G NR to 802.11p. The whitepaper by 5G Automotive Association [10] presents some benefits of using the 5G phys-

ical layer in V2X communications. They define three types of cellular connections: device-to-device (direct communication, similar to 802.11p), device-to-cell tower and device-to-network. The authors explain that many concepts, such as mobile network operators (MNOs), can be reused from the current cellular communication structure in the future V2X. MNOs will provide, among other things, data security and privacy mechanisms already existing in cellular networks. Further in the paper [10], a table showing the advantages of C-V2X over IEEE 802.11p is presented.
In [21], Boban et al. also discuss the physical layer of 5G V2X. They define three types of cellular connections: cellular V2X, cellular-assisted V2V and cellular ad-hoc V2V. The last one is similar to 802.11p, but better in spectrum usage and initial access procedure. It can be used in out-of-coverage scenarios and still be synchronized, using GNSS and by synchronizing with in-coverage users. Multiple radio frequencies within a single band will make the links more robust and offers flexible frequency usage. Better network capacity and a broader spectrum are achieved by reducing the cell sizes and because of this, mmWave radio technology becomes more interesting. But it is restricted to a short range and line-of-sight (LoS) communication. Also, a special frame design and numerology are needed to reduce the Doppler effect. IEEE 802.11p, on the other hand, is resistant to the Doppler effect and has a low latency thanks to the short frame.

2.5 5G New Radio

As shown in Subsection 2.4.6, 802.11p and C-V2X have different pros and cons. The next generation cellular networks, 5G, will introduce a new radio technology, called NR. NR is being developed with different kinds of communications in mind from the very beginning (e.g., V2X). The first release of the 3GPP NR was ready at the end of 2017 [2]. It is expected to provide much faster and more reliable communication, using a much broader bandwidth. Many different new technologies are being proposed for the 5G physical layer, such as millimeter wave (mmWave), massive MIMO, NOMA, cognitive networks and Visible Light Communication (VLC) [75]. These key concepts will be presented in this Section.

2.5.1 mmWave

Current LTE radio has a maximal frequency of 2.6GHz, but there is a rising need for higher data transmission rates and broader bandwidth. To support this, the new mmWave technology will be introduced, to provide a frequency spectrum of 30-300 GHz by using a wavelength as short as 1-10 mm [22]. Thanks to the decreasing wavelength, also the antennas can be decreased in size.
Unfortunately, the very short wavelengths also introduce new challenges, as they are sensitive to rain and humidity as well as blocking buildings and trees. Because of this, mmWaves require more-or-less line-of-sight (LoS) conditions [22]. As a countermeasure that will partly solve these problems, 5G NR will include a multi-node beamforming technology that is presented in the next Subsection.
Another problem is the short coverage of mmWaves, which is around one kilometer. This will be solved by more dense installation of small-cell base stations and beam-

forming. This in turn introduces new privacy challenges, discussed in Subsection 2.3.3.

2.5.2 Massive MIMO and beamforming

In order to enable reliable mmWave technology and counter the signal fading problems, a new beamforming technology is introduced. The decreasing antenna size enables the installation of multiple small antennas at each base station. These massive multiple-input-multiple-output (MIMO) antenna arrays in their turn, enable the formation of narrow beams that can be aimed at individual users (see Figure 2.9). Using beam training and beam tracking, a beam can then follow a given user to provide continuous communication through the same link.

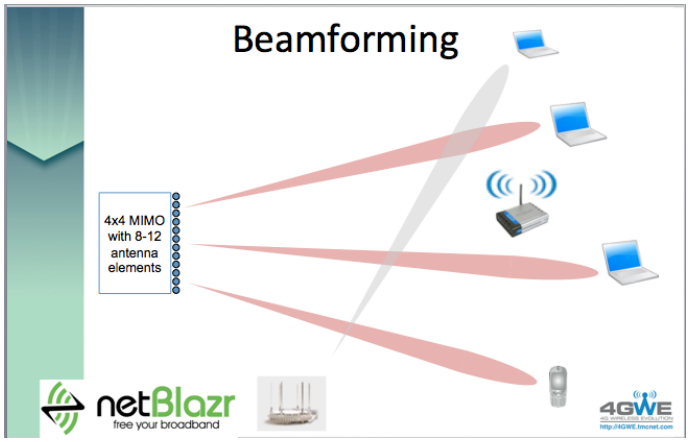


Figure 2.9: A visualization of how beams can be formed using massive MIMO antenna arrays

These technologies have also been studied in connection to V2X communication. In their paper [81], Va et al. present a beam tracking solution for faster beam training required by highly mobile devices (e.g., cars). In the presented method a single beam pair is trained to track a path, instead of many beam pairs as presented in previous papers. This is possible thanks to beam tracking, where an extended Kalman filter was used as a tracking filter because of its low complexity. The same topic is investigated in [67], where Larsson et al. implement efficient beam tracking in high-speed scenarios with frequent switches between transmission points. They performed experiments on a BMW race track that showed good results. They also emphasize the need to handle big Doppler shifts introduced by the high speeds. In [79], Tateishi et al. also present a solution for user mobility with a narrow beam. They use channel state information (CSI) to choose the best beam for minimal signaling overhead.
In the paper [32], Duan et al. propose an architecture for Vehicular Ad-Hoc Networks (VANETs). It includes vehicle clustering with 802.11p between vehicles in the cluster and 5G beamformed transmission between the cluster head (CH) and the cellular base station. This clustering method reduces signaling overhead between vehicles

and the base station. SDN is used to separate the data plane from the control plane and thus: "...facilitates the centralized control over HetNets by providing a global network view and a unified configuration interface despite the underlying HetNets involved."
The beamforming and beam tracking technologies provide new possibilities also in terms of security. In [88], the authors Yaacoub and Al-Husseini present a method for providing PLS by using beamforming. They explain that previous PLS solutions used trusted relays to introduce jamming for potential eavesdroppers. However, the presented new method avoided this by using MIMO beamforming from source to destination, with "built-in" jamming. In another paper [92], Zhao et al. instead present a method for secure communication over an untrusted relay, in the case when relaying is actually necessary for amplifying a signal. The two-way communication supports full-duplex operation and MIMO signaling. In another paper [15], Al-Momani et al. propose to use beamforming in order to enhance physical layer (re)authentication. The authentication (also mentioned in Subsection 2.3.3) uses a so-called unique channel "signature", consisting of variations in Doppler shift, etc. The beamforming technique can be used to enhance this method, which can enable physical layer authentication in terms of sender location.

2.5.3 NOMA - non-orthogonal multiple access

Another important method that might be used in 5G NR is non-orthogonal multiple access (NOMA) [66]. This is a scheduling method that can be compared to such well-known methods as frequency division multiple access (FDMA), time division multiple access (TDMA) or code division multiple access (CDMA). All of these previous methods are called orthogonal multiple access (OMA) methods and fail to support the high data rates required for 5G NR.
In NOMA, multiple users can transmit at the same frequency and in the same time slot. The signals are transmitted together in one waveform and then separated at the receiver by power level. The entity performing the separation is called the successive interference cancellation (SIC) receiver. The reason it is called successive, is that the separation is performed iteratively: the strongest signal is extracted and subtracted until the right signal is found.
The technology provides significantly higher data rates, spectral efficiency (SE) and energy efficiency (EE) than e.g., orthogonal FDMA (OFDMA), when perfect cancellation at the SIC is assumed. However, perfect cancellation is very hard to achieve in reality and it is more probable that some interference between the signals will remain. As could be expected, the more interference remains, the lower the data rates get. Unfortunately, cancellation errors are quite probable in fading channels. Another problem with NOMA is that high computational power is required to run SIC algorithms, especially when the number of users increases and high data rates are required. Also, power allocation optimization will be a challenge for highly mobile users, such as vehicles. In order to counter these problems, NOMA can be combined with MIMO to provide better reliability and less decoding errors.
In their paper [75], Satrya and Shin discuss another problem with previous NOMA schemes, namely a privacy vulnerability. They claim that the iterative separation at

the SIC enables a malicious user to extract the messages addressed to other users. They also propose a solution to this, by using one key for hashing and another one for authentication. The first key will ensure that a legitimate user is performing the decoding. The second key consists of the user's MAC and IMEI embedded in the device. It is used to ensure it is the user with the right MAC and IMEI that tries to decode the message. However, this paper does not include an analysis of how this secured scheme will effect the data rates.
Xu et al. have published two papers about two different schemes to enhance physical layer security in NOMA. In [86], a relay network is assumed, where a user with better channel conditions may serve as a relay for a user with worse channel conditions. In this case, the authors propose a solution to protect the data of the served user from being eavesdropped by the relaying user. The scheme is designed for Spectral Efficiency Improvement and Eavesdropping Suppression (SEIES). In their other paper [87], the authors explain the same privacy vulnerability as Satrya and Shin [75], and propose another scheme called Eavesdropping Suppression by Full-Duplex Technology and Signal Transformation (ES-FDST). In both of the papers by Xu et al., it is shown through performance analysis that the schemes are feasible and improve security.

2.5.4 Cognitive radio networks

Cognitive Radio (CR) is an intelligent radio that can better utilize the radio spectrum [77], [85], [83]. It enables unlicensed users to coexist with licensed users by using different parts of the spectrum. The licensed users are seen as primary users and have a higher priority. The unlicensed (secondary) users on the other hand, only get to transmit when there is a spectrum hole, i.e., a part of the spectrum is unused by primary users during a period of time. This kind of spectrum-sensing intelligent radio can be achieved using Software Defined Radio (SDR), which is more flexible than the traditional hardware implementation [77].
This new technology improves throughput and capacity, but its complex nature also enables many new attacks, primarily aimed at the network availability [77].
Another security concern with the introduction of this new technology is confidentiality. Many different PLS solutions have been proposed and among these, a PLS solution for transmission protocols in CR networks (CRN). Due to the coexistence of primary and secondary users at the same bandwidth, there is a high risk for a secondary user eavesdropping on a primary user [85]. The authors Xie et al. add artificial noise to the original signal through Superimposed Coding (SC), which causes interference at a potential eavesdropper. The noise is generated from a pseudo-random sequence that is known to the sender and the receiver, but not to the eavesdropper. Simulation and numerical results show an increased security for primary users, as well as better outage performance for secondary users.
In [83], Wang et al. present another solution called a Prioritized Secondary User Access Control (P-SUAC) technique, where secondary users are divided into authorized and unauthorized. In the absence of primary users, authorized secondary users (A-SUs) are allowed to exchange messages with an additional jamming pattern, which is unknown to the unauthorized secondary users (UA-SUs). The A-SUs

are further divided by priority level by introducing an imperfect projection method.

2.5.5 VLC - visible light communication

Last but not the least, there is an active research going on around visible light communication (VLC). This is actually not a part of 5G NR, but rather an alternative to radio transmission. Research in this field has been going on for a long time, with early implementations such as the RONJA project in 2001 [9]. However, quite recently this technology was proposed for future 5G implementations. VLC enables data transfer by flickering the light of a LED (or laser) at speeds much faster that the human eye can perceive. When the light is turned off, this represents a 0-bit and respectively when it is turned on, it represents a 1 [65], [23].
In [91], Zhao et al. demonstrate a VLC system that could be useful for backhaul communication, i.e., between the small cell towers and the network core. Its benefits in a long-distance outdoor VLC system are presented. The authors also discuss the benefits and drawbacks of VLC. On the one hand, it is a green technology and more cost-effective than mmWave. It has the same capital-expenditure, operating expense advantages as mmWave, but requires cheaper devices. Drawbacks include low Signal-to-Nose Ratio (SNR), that light diverges significantly at long distances, channel fading and sensitivity to ambient noise (especially outdoors).
In another paper [82], Valiveti propose a system for LiFi/WiFi hybrid communication for passengers in high speed trains. The system combines a so called "grey system" with a neural network to decide when handover between LiFi/WiFi APs should take place. The decision is made by measuring the Signal to Interference Ratio. The authors also present several other benefits of LiFi, in this case compared to WiFi. The use of LiFi is motivated by the fact that it has a broader spectrum range than the WiFi radio spectrum. The authors also claim that LiFi has a higher power efficiency than WiFi. On the other hand, VLC requires LoS conditions.
In their paper [65], Karthik et al. propose a cost-effective system for voice communication between two car drivers using VLC. The communication between the two users is two-way and authenticated. A drawback is once again that the system requires LoS between the cars.
Research has also been going on for implementing VLC in V2X communication. Cailean and Dimian present in [23] the pros and cons of VLC in automotive implementations. The authors emphasize the low cost, gradual integration of LED light sources and the high accuracy positioning services. Another benefits are the high packet delivery ratio and low latencies. This is due to the implicit light features, which prevent severe multipath effects, mutual interferences and Doppler spread. On the other hand, V2X applications also require long-distance transmission as well as the ability to cope with bad weather conditions. This is currently problematic for VLC. One of the main problems is interference of ambient light, e.g., sunlight, artificial light.
A system is presented where information is broadcasted to vehicles through light signals. The vehicles then forward the information together with their own status, using their head and tail lights. The authors also discuss different receivers. Camera-based VLC receivers require high speed cameras for acceptable performance, which

is too expensive. Also all cameras have a frame rate that is not fast enough, i.e., light flickering at the corresponding rate can affect the human eye. Another type of receivers are based on photodiodes and offer high sensitivity and linear response. This type of receivers has a quick response and is thus suitable for high speed communications.

3
Analysis

In the previous chapter, standards and research papers were presented in the studied area, i.e., how the introduction of the new radio technology of 5G in V2X communications will affect the security of the current standards. In this chapter the knowledge gained from the literature study is used to answer the research questions posed in the beginning of this report. The questions to be answered are the following:

- RQ1: What protocols and security mechanisms have been used this far in ETSI V2X communications?
- RQ2: What are the security requirements for the different ETSI ITS use cases?
- RQ3: Which features of 5G NR can be used to improve security at the physical layer? Could some security mechanisms be simplified or entirely removed from higher layer protocols?
- RQ4: What new vulnerabilities could 5G NR bring to the V2X communication?
- RQ5: Is it possible to exchange 802.11p with 5G NR with no or minimal changes to the higher layer protocols? If not, what are the obstacles?

Each of these research questions will now be discussed and answered one by one in the following Sections of this analysis.

3.1 RQ1: Security in ETSI V2X communications

This question has already been answered in the beginning of the survey, i.e., in Section 2.1. The findings of this part of the survey will now be summarized and the security mechanisms used in ETSI ITS will be briefly explained. Also the security aspects that these mechanisms guarantee will be presented.

SecuredMessage The SecuredMessage packet consists of payloads, which are primarily CAM or DENM, and the different headers and trailers that the Security layer require. The SecuredMessage header contains a protocol version as well as the *security profile*. The security profile is used for the encoding of the message and specifies the message format as well as mandatory header, payload and trailer fields.

Confidentiality The security profiles for CAMs and DENMs state that these messages shall not be encrypted [52]. As the analysis will show in the following Sections, data confidentiality is actually not a problem in most of the use cases in the Basic Set of Applications. However, during authentication of a user by a certificate authority, the credentials exchanged are cryptographically encrypted using a public

key [45].
Integrity and Authentication In the ETSI ITS model, cryptographic signatures are used to authenticate the sender and guarantee the *integrity* of the message [45]. The message is signed and verified using either symmetric or asymmetric cryptography.
Privacy By using temporary pseudonyms instead of the permanent identifier, privacy of the sender is guaranteed, i.e., the user cannot be tracked. The pseudonyms should be regularly updated [49] and it should be impossible for an attacker to link the pseudonym to the canonical user identity [45].
Availability The ETSI ITS security documents do not explain much about guaranteeing availability for the messages. In [45], availability is mentioned in a table with corresponding solutions. Some of these are "Include source address in all V2V messages", "Limit message traffic to V2I/I2V where possible" and "Include a sequence number in each new message".
Certificate structure In order to distribute and validate asymmetric keys for encryption and signatures, a certificate structure is required. The Certificate Authorities (CAs) that are responsible for granting certificates are structured in a hierarchy. At the top is the "ultimate root of trust" [50] called Root CA and below are the Enrollment CA and the Authorization CA. The Enrollment CA is used for initial authentication and provides a pseudonym to the user. Then the Authorization CA gives the user permission to perform certain requested operations.

3.2 RQ2: Security requirements for ITS use cases

Right now, the same security mechanisms apply to all CAMs and all DENMs, respectively. However, the different use cases presented in the ETSI ITS standard [43] have different security requirements. In this Section, the different requirements are presented and motivated. For every application/ specific use case, the requirements were studied for the CIA model (*confidentiality*, *integrity* and *availability*) as well as two other aspects: *privacy* and *authentication*. The results of this analysis can be seen in Table 3.1. Finally, the findings are summarized and three use cases are chosen for a deeper analysis in the following Sections.

3.2.1 Active road safety

The Active road safety group consists of use cases that are critical in terms of reliability and low-latency, since they are used to guarantee road user safety.
Availability: This application class has strict requirements on *availability*, since the safety warnings have the highest priority and have to be delivered as soon as possible.
Confidentiality: On the other hand, *confidentiality* is not as important for these messages, since the warnings are sent to everyone who might be affected by the danger and do not have to carry any sensitive data.
Integrity: *Integrity* is also important for safety messages, since a modified message might mislead the vehicle to behave in a dangerous way. To demonstrate this, imagine a vehicle sending the Slow vehicle warning. If this message is modified to

say something less urgent, such as Point of Interest notification (which is also a CAM message), this might cause a serious road hazard.
Authentication: The requirements for *authentication* varies among the different use cases. For warning messages initiated by normal vehicles, *authentication* is only required by the receiving vehicles in terms of location. According to the receiving users, there is no need to supply the actual identity of the issuing vehicle, since it does not really matter who sent the message as long as it can be proven that the sender was really at that location. On the other hand, it might be needed for audit purposes, i.e., to identify repeatedly misbehaving users.
Another question that could be asked is whether it is profitable for a user to falsify the identity? In many of the road safety cases, the attacker sending out a fake warning causing an accident could be hurt in the accident himself. Such an attack could only be profitable to perform from a safe distance, but in that case the receivers would notice that the sender has another location (through location *authentication*). Because of this, full *authentication* is redundant in such use cases as Slow vehicle indication, Lane change and different Collision warnings.
For special vehicles however, there is a need to *authenticate* which kind of vehicle issued the warning, e.g., if the Emergency vehicle warning was really initiated by an emergency vehicle. The same applies to the Roadwork warning, the Motorcycle approaching indication and also the Collision warning, sent by a vulnerable user (e.g., pedestrian) or RSU.
Privacy: When it comes to *privacy*, the requirements vary even more and the answer is not always clear. For the Emergency vehicle warning, Slow vehicle indication, Motorcycle approaching indication and Co-operative glare reduction, *privacy* is important to protect, since these messages are sent out regularly during the trip and can thus be used to track a user. Also in the case of Collision warning issued by a vulnerable user, there could be a *privacy* risk if the vulnerable user remains at risk during a long period. With the Overtaking vehicle warning and Lane change assistance, *privacy* might be a problem if the overtakes or lane changes are frequent. The other cases consist mostly of temporary road hazard warnings and thus cannot be used for tracking a user (i.e., *privacy* not that important). In the case of Signal violation warning, the message is sent by an RSU, so *privacy* is not important here either.

3.2.2 Cooperative traffic efficiency and local services

These two application classes are less safety critical and include Speed management, Parking management and Media downloading.
Availability: These applications have in common that they are less time critical and can thus have a lower priority than the Active road safety applications.
Integrity: *Integrity* is important to some extent, but less than in the case of Active road safety since the information is not as critical for safety.
Authentication: Another common feature is that the messages are sent by the RSU to surrounding vehicles. This implies that proper *authentication* of the RSU has to be done.
Privacy: Also it implies that in most of the cases, *privacy* is not important, since

the sender is not a private vehicle.

Confidentiality: *Confidentiality* is not that important either, since the RSU (in most of the cases) sends out the same information to all bypassing vehicles.

There are some exceptions though, e.g., Automatic access control/parking management and Media downloading. In these cases, the user responds to the RSU with credentials and thus *confidentiality* and *privacy* become important, as well as *authentication* of the user. Other special cases are Adaptative cruise control and Highway automation system (platoon). Since the messages are sent continuously by moving vehicles, *privacy* becomes important. Since communication is required between a restricted set of vehicles (especially in a platoon), best practice would be to set up a completely secured channel between these. This would include the entire CIA model as well as *privacy* and *authentication* of all the involved vehicles.

3.2.3 Global internet services

This group consists of applications requiring access to the global network. Some such services are Fleet management, Stolen vehicle alert and Remote diagnostics.

Confidentiality, integrity and authentication: Since this group consists of applications that require either the RSU or the vehicles to access the global network, good security is required here. More specifically, *confidentiality*, *integrity* and *authentication* are critical in all of the cases.

Availability: On the other hand, *availability* might not be of primary importance, since the messages are not safety critical (at least not in real time).

Privacy: *Privacy* is important in most of these cases, since otherwise the user might be tracked or some personal data might be associated to the identity (e.g., Insurance and financial services). In the case of Loading zone management, *privacy* is important because an attacker might associate the identity with a certain loading time. However there are several cases when *privacy* is not as important, i.e., Stolen vehicle alert, Vehicle software/data provisioning/update and Vehicle and RSU data calibration. The Stolen vehicle alert is sent by the stolen vehicle itself and is used to track the vehicle, so *privacy* is thus not important here.

3.2.4 Summary

The use cases together with their security requirements are shown in Table 3.1. It can be noted that the safety critical cases mostly require *integrity* and *availability*, while the other cases require *integrity* and stricter *authentication*. *confidentiality* and *privacy* are required by less use cases, especially in the road safety group.

Applications Class	Application	Use case	C	I	A	Privacy	Auth.
Active road safety	Driving assistance - Cooperative awareness	Emergency vehicle w.					
		Slow vehicle indication					
		Intersection collision w.					
		Motorcycle approaching ind.					
		Overtaking vehicle w.					
		Lane change					
		Glare reduction					
	Driving assistance - Road Hazard Warning	Emergency electronic brake lights					
		Wrong way driving w.					
		Stationary vehicle					
		Traffic condition w.					
		Signal violation w.					
		Roadwork w.					
		Collision risk w.					
		Dec. floating car data					
		Collision unavoidable					
Cooperative traffic efficiency	Speed management						
	Cooperative navigation						
	Other	Platooning					
		Adaptative cruise control					
Cooperative local services	Location based services	Point of Interest notification					
		Automatic access control/ parking management					
		local electronic commerce					
		Media downloading					
Global internet services	Communities services	Insurance/financial services					
		Fleet management					
		Loading zone management					
	ITS station life cycle management	Vehicle software/data provisioning and update					
		Vehicle-RSU data calibration					
	Other	Instant messaging					
		Personal data synch.					
		stolen vehicle alert					
		Remote diagnosis					

Table 3.1: ITS use cases and their security requirements (red = strict, yellow = intermediate, green = not required)

3.3 RQ3: 5G New Radio security solutions

The new security possibilities that will be introduced with 5G (implicit and explicit) are analyzed for three chosen use cases. These three cases are Emergency vehicle warning, Collision risk warning and Decentralized floating car data. The first case is interesting because the message is sent by a special kind of vehicle. The Collision risk warning is interesting because it can be sent by different users and also by RSUs. Finally, the Decentralized floating car data is interesting because of the *availability* risks it creates, which were described earlier. Finally, the redundant cryptographic mechanisms are discussed.

3.3.1 Solutions provided by 5G NR implicit security

As can be seen in the table, *integrity* is required in all three of the cases. *authentication* is mainly required by the receivers in terms of location of the sender (except in the case of the Emergency vehicle warning, where a proper identity authentication is required). At the same time, the identity is needed for authorities to track continuously misbehaving users.

Physical layer authentication Location *authentication* can be done on the physical layer, using the physical layer *authentication* technology discussed earlier in Subsections 2.3.3 and 2.5.2. Further, beamforming can be used to enhance this technology and make it even harder for an attacker to guess or manipulate the unique location-dependent channel signature.

This technology would be enough for the Collision risk warning use case. However, this is not enough for The Decentralized floating car data, since the sender does not have to be at a certain location (the message gets repeated from one vehicle to another to spread over a greater distance). Also the Emergency vehicle approaching will need full authentication, as discussed earlier in Subsection 3.2.1.

Even if channel response fingerprinting does not replace the cryptographic *authentication* completely, it can be used to offload the communicating nodes (as described in [15], Section 2.5.2). In this case, the cryptographic mechanisms can be used for initial *authentication* between two users. After that, the repeated (CAM) messages can be (re)authenticated using physical layer *authentication*. In this way, less cryptographic computations have to be performed, which is an important improvement for latency critical systems.

Integrity by channel response fingerprinting If physical layer *authentication* can be implemented, this will also enable physical layer *integrity*. In order to understand this, imagine a scenario where an attacker wants to modify a message, i.e., attack the *integrity* of the message. In this case, the attacker has to first intercept the message, then modify it and finally re-send it to the destination. Assuming physical layer *authentication* is used, the location of the attacker will be revealed to not match the expected location of the sender. This will show that there has been an attack and the message was not sent by the expected user.

The above discussed technology would solve the *integrity* and *authentication* required by most of the safety related use cases and specifically two out of our three chosen cases. Nevertheless, the Emergency vehicle warning that is our third chosen

case, requires stricter *authentication*. This cannot be solved by the physical layer *authentication* and requires cryptographic mechanisms.

Availability through NOMA and cognitive radio *Availability* is required by all of the three cases and actually by all of the road safety critical use cases in general. The Decentralized floating car data implies a special risk for *availability*. Since the messages in this use case are repeated from one car to another (in order to spread the warning over a greater distance), an attacker might trigger multiple such message "waves". This could potentially result in a message flood that jams the network and thus disables legitimate users to get network access. For this reason it is important to introduce security mechanisms that will prevent this type of attack. In order to provide better *availability*, NOMA scheduling and cognitive radio networks can be used. These technologies, discussed in Subsections 2.5.3 and 2.5.4, provide better resource utilization and therefore contribute to a more available network.

Privacy in the three chosen use cases The *privacy* requirements are different in all three chosen use cases. In the case of the Emergency vehicle warning, the emergency vehicle might be tracked by the repeatedly sent out messages. The question is if this could be used for malicious intents, since the *privacy* of an official vehicle's location might not be as urgent as the *privacy* of a normal road user's location. In the case of the Collision risk warning, *privacy* might be at risk for a vulnerable road user, e.g., a pedestrian, who is in a continuous danger, e.g., walks through a dangerous area. Then once again, the messages will be sent out continuously and the user can be tracked. On the other hand, if the user is in danger for life maybe the *privacy* is not of primary importance. In the case of Decentralized floating car data, *privacy* is not important, since the messages are only sent by each vehicle for a short period of time and can thus not be used for tracking purposes.

After discussing the *privacy* aspect of each of the three chosen use cases, it can be concluded that *privacy* is not of primary importance for these.

Confidentiality *Confidentiality* is not a problem in those cases either, because none of the road safety messages carry any sensitive user data. This is also probably the reason why the security profile of CAMs and DENMs (ITS) state that these messages shall not be encrypted [52]. Nevertheless, it should be noted that in some use cases *confidentiality* is actually important, e.g., in the Automatic access control/parking management use case. For those cases, *confidentiality* might be guaranteed by using the mmWave and beamforming technologies as described in Subsections 2.5.1 and 2.5.2.

3.3.2 Other 5G security technologies

As shown in the previous Subsection, *authentication* and *integrity* can be solved to some extent implicitly by using channel signatures. However, as can be seen in Table 3.1, the chosen use cases also require *availability* and (for the Emergency vehicle warning) *privacy*. This Subsection discusses explicit security solutions for these requirements, as well as mentions some solutions for the aspects that are of less importance.

Availability: Availability can also be partly solved implicitly, as shown, but there

are methods than can improve the *availability* even further. These include the solution presented by Bian et al. [20], i.e., a special channel hopping process can be established to avoid jamming. The two communicating parties hop between channels in a sequence unknown to the attacker (see Subsection 2.4.4). Other solutions include a new packet forwarding approach to avoid flooding and message storms introduced by broadcasts, as well as letting vehicles with a better connection serve those with a worse connection to the RSU.

Privacy: *privacy* is not critical for the three chosen use cases, as was shown in the previous Section. Nevertheless, *privacy* can be partly solved by randomizing choice of base station, as shown by Farhang et al. (see Subsection 2.3.3). Another way to provide *privacy* is through distributed knowledge, where different information about a user is distributed among different entities.

Confidentiality: There are many methods to solve *confidentiality* through PLS (see Subsection 2.3.3), but in the three chosen use cases *confidentiality* is not important. This can however be used in such cases as the Automatic access control/parking management and instant messaging.

Authentication: Whenever the vehicle is within network coverage, the *authentication* provided by 5G core network can be applied. The 5G-AKA protocol (see Subsection 2.3.2) can be applied for any UE with a USIM and that is able to connect to a base station. This 5G technology is enough to fully authenticate a user to the network and leaves the ETSI ITS authentication mechanisms redundant for in-coverage users. Because of this, it is necessary to compare the two technologies and choose the most efficient one for V2I communications.

Unfortunately, very little information has been found in the literature about 5G-AKA authentication for UEs that are out of coverage. As a consequence, it cannot be stated that 5G-AKA can fully replace the ETSI ITS authentication. Therefore, other technologies may be used for direct link authentication, such as a combination of the mechanisms in the ITS model and the physical layer authentication proposed in the previous Section.

Identity-Based Cryptography: The analysis shows this far that in certain cases cryptographic signatures may still be needed. This implies that also asymmetric keys are needed. Nevertheless, the certificate infrastructure used to manage certificates can be avoided by using IBC (see Subsection 2.4.5). By enabling each user to generate the public key of any other user from his identity, key verification becomes unnecessary. This technology has already been studied by many papers for IoT [73][31][17] and mentioned in a Huawei whitepaper [40] as a solution for V2X as well.

3.3.3 Redundant cryptographic mechanisms

The above Subsections show that the most important security aspects for the three chosen use cases are *integrity*, *authentication* and *availability*. It has also been demonstrated that there are physical layer technologies available for 5G, that can provide solutions for these aspects.

The cryptographic signatures become redundant to some extent in all of the use cases where the receiver require *authentication* only in terms of location. This can be

solved instead by channel signatures. *Encryption* is not required in the three chosen use cases. As shown in [72] and [15], physical layer *authentication* can be combined with cryptographic *authentication* in the higher layers to achieve full *authentication* (i.e., location and identity).

The above argumentation shows that the cryptographic keys and the certificate infrastructure are only required in certain cases. More specifically, for the cases requiring full authentication and when authorities need to be able to track misbehaving users. Furthermore, the certificate infrastructure might prove to be redundant, if the IBC technology discussed in the previous Section can be implemented for vehicles. Since previous papers mostly discuss IBC for IoT, some adjustments would be needed for V2X instead. Nevertheless, this seems to the author to be a very promising technology for the future and might optimize the cryptographic mechanisms to a great extent.

3.4 RQ4: 5G New Radio vulnerabilities

The new security solutions presented in the previous Section will solve some of the security requirements and replace the corresponding mechanisms in the ETSI ITS model. Nevertheless, the new technologies introduced with 5G NR have vulnerabilities that security analysts and OEMs should be aware of and handle accordingly. The following Section presents these vulnerabilities, along with possible solutions found during the survey.

Privacy Many of the new technologies of 5G NR presented in this paper could have a negative impact on *privacy*. The small cells introduced to enable the mmWave make it possible for an attacker to draw conclusions about the location of a user from his choice of base station. This can be countered by adding some randomization to the choice of base station, as described in the previous Section, as well as in Section 2.3.3. As previously explained in Section 2.5.2, the beamforming technology can bring *privacy* problems, because beam tracking implies tracking a user.

Also NOMA might introduce *privacy* issues if not handled correctly, because the receiver extracts the strongest signal iteratively and thus extracts signals with other destinations (see Section 2.5.3). To solve this, it should not be possible for a non-legitimate receiver to translate a signal to the sent message.

Availability Cognitive radio might introduce *availability* problems, due to its complex nature (Section 2.5.4). There are some papers though that propose methods to secure cognitive radio implementations.

Confidentiality The cognitive radio might also introduce *confidentiality* issues. That is why several papers study different solutions for *confidentiality* in cognitive radio, as described in Section 2.5.4. One of these is introducing noise to possible eavesdroppers while keeping the channel between sender and authorized receiver intact. This approach is very similar to PLS.

3.5 RQ5: Exchange 802.11p with 5G NR

One of the research questions posed in the beginning was if the replacement of 802.11p with 5G NR can be done smoothly. The short answer is yes, since NR is not defined yet and could therefore be developed as needed. Due to the modularity of the network stack, the higher layer protocols should not be affected by the change of transmission frequencies or another scheduling method (NOMA).
As already mentioned in Subsection 2.4.6, since 5G NR is still under development, it is hard to compare its features to the IEEE 802.11p protocol currently used in the ETSI ITS model. Instead, the 802.11p protocol is compared to the already standardized technology of C-V2X. In Subsection 2.4.6 a summary of the basic features of the two technologies was shown in a table. According to those basic features, the C-V2X and 802.11p are actually quite similar. However, after studying the research papers described further in the same Section, it was found that there are really several differences. These are summarized in Table 3.2, which shows the benefits vs the drawbacks of using C-V2X instead of 802.11p.

Benefits	Drawbacks
More efficient when the loads increase, i.e., in urban areas	Stricter requirements on synchronization
Has an infrastructure for scheduling and load balancing (less collisions)	Worse at handling collisions
Global infrastructure solves the hidden node problem	The near-far problem is introduced
Resource allocation more flexible	Vulnerable to the Doppler effect
Longer coverage	Less adapted to out-of-coverage scenarios (synchronization)
	Big frame –> bad at transmitting small amounts of data
	More sensitive to frequency errors
	No USIM for motorcyclists

Table 3.2: Benefits and drawbacks of using C-V2X instead of 802.11p

As can be seen in the table, the drawbacks of C-V2X outweigh the benefits. However, some of these problems have already been solved in 5G V2X.
The Doppler effect, which in C-V2X becomes a problem when vehicles are moving at high speeds, is solved in 5G by using *dual connectivity*. This means a connection to both a 5G NR base station and an LTE eNB simultaneously [74]. The near-far problem is worsened when there is an overlap between signals [13], which are introduced by, e.g., Doppler shifts. Since the Doppler effect has been solved in 5G, this also reduces the near-far problem.

4
Future work

As the results of the analysis demonstrate, the cryptographic signatures used for ETSI ITS can become redundant if the USIM and the 5G-AKA protocol are used. In certain circumstances (e.g., fast re-authentication) it can even be enough to use the channel response fingerprint. Also the new 5G technologies, e.g., mmWave and beamforming, can help to improve the different aspects of security. This chapter presents different directions for future research in the field.

4.1 Comparing 5G-AKA and ITS authentication

A very relevant question is which of the two authentication technologies used in 5G vs the ITS model is more efficient in V2X communications. The two technologies can be compared in terms of speed and resource utilization, as well as which technology is best suited for moving users. Another question that is interesting to investigate is how the 5G-AKA protocol is used for out-of-coverage users. Since the protocol requires a link between the vehicle and a base station, as explained earlier, future research should be aimed at finding how to enable authenticated communication between vehicles through a direct link. The same problem appears in the ITS model, where certificate verification requires a link to a certificate authority. As opposed to smartphone users, vehicles require a continuous connection to enable road safety.

4.2 Channel response reliability and integration

Further, channel response can be used to enable a faster authentication. Even though this technology does not directly authenticate a sender by the identifier, it can still be used for e.g., re-authentication in repeated warning messages. This is possible assuming authorities do not need identity authentication in every sent message for audit purposes.
In order to apply this technology, it first needs to be verified as trustworthy and reliable. An important issue to be taken into consideration is whether the changing environment can change the fingerprint. It also has to be verified that channel fingerprinting is possible with moving senders and receivers. Privacy problems have to be analyzed thoroughly and in case these pose a serious threat to users, countermeasures have to be found. Further, beamforming can be used to improve the precision of physical layer authentication. Finally, the technology can be integrated into the existing ITS model. An important part of the integration is that the phys-

ical layer authentication has to be combined with the cryptographic mechanisms and/or 5G-AKA in a seamless way.

4.3 Adapting IBC for V2X communications

As has been explained earlier, IBC can be used to remove the need for certificates in the ITS model. The technology would simplify the key verification process and enable direct authentication, without the need to contact a certificate authority. Further, if this is used in the ITS model, this may improve the ITS authentication to such a degree that it will outweigh the 5G-AKA for V2X.
The IBC technology brings a lot of benefits, but on the other hand it still has to be adapted to V2X communication. The idea for such a cryptographic system was presented a long time ago and currently it has been adapted for IoT systems. Since IoT is (to some extent) similar to V2X, it is very likely that IBC can be adapted for V2X as well. Nevertheless, there is a need for research in this area before practical integration is possible.

4.4 NR technologies to improve availability

Some of the new technologies that are proposed for 5G will bring new possibilities to improve availability. Among these are the NOMA scheduling and the cognitive radio. NOMA scheduling enables transmitting several signals in the same frequency at the same time, while the cognitive radio provides a better resource utilization by sensing the network. Both of these technologies, if implemented correctly, can improve the network availability. However, the implementation must be made secure, since NOMA might introduce privacy issues and cognitive radio has a complex nature that can be exploited by different attackers. This implies that there is a need for further research about these technologies in V2X before the actual integration is possible.

5
Conclusion

In this report, we present a literature study together with a corresponding analysis of how 5G will affect the security of V2X communications. Firstly, the current standards for V2X communications, with focus on the ETSI ITS model and its security, are described. Further, the security solutions in 5G are discussed. In the analysis, the security requirements of different use cases are presented, along with corresponding solutions. The security aspects investigated were confidentiality, integrity, availability, privacy and authentication. It was found that for authentication, the heavy cryptographic algorithms in ITS can be replaced by the 5G-AKA protocol (if it proves to be more efficient) and physical layer authentication. Moreover, the certificate infrastructure of the ITS model can be removed entirely, if IBC will be adapted for V2X communications. Finally, different directions for future work in the field are described.

V2X communications have been studied since long before the development of 5G. The protocol stack and security mechanisms in ETSI ITS were standardized from the state-of-the-art technology of that time. However, the development of 5G is rapidly advancing, with new standards and proposals published even during the writing process of this thesis. Due to the new speeds and other technological novelties in 5G, many researchers and people in industry anticipate that 5G is the future technology for V2X communications. Consequently, it is essential to thoroughly analyze the security of 5G and how it can be integrated into the current ITS model. This is a very broad field that brings many new aspects for future research.

Bibliography

[1] The 5G-ENSURE Project. URL http://www.5gensure.eu/, visited 2018-02-14.

[2] 5G NR timeline. URL http://www.3gpp.org/release-15, visited 2018-05-25.

[3] The 5G-ENSURE test-bed for 5G at bcom in Rennes. URL https://5gensure.eu/news/bcom-test-bed-showcase-9th-international-cyber-security-forum-2017, visited 2018-02-14.

[4] The Vinnova/FFI BAuD project. URL https://www.vinnova.se/p/baud-storskalig-insamling-och-analys-av-data-for-kunskapsdriven-produktutveckling/, visited 2018-04-25.

[5] The ChaseOn MANTUA project. URL http://www.chalmers.se/en/centres/chaseon/research/Pages/Multiantenna-wireless-architectures-for-next-generation-wireless-systems-%E2%80%94-MANTUA-.aspx, visited 2018-04-25.

[6] The Vinnova/FFI HoliSec project. URL https://www.vinnova.se/p/holisec-holistiskt-angreppssatt-att-forbattra-datasakerhet/, visited 2018-04-25.

[7] The mmMAGIC project. URL https://5g-mmmagic.eu/, visited 2018-04-25.

[8] The 5GCAR project webpage, 2017. URL https://5gcar.eu/, visited 2018-02-18.

[9] Ronja - reasonable optical near joint access, a project of optical point-to-point data link, 2017. URL http://ronja.twibright.com/, visited 2018-03-08.

[10] 5G Automotive Association. The Case for Cellular V2X for Safety and Cooperative Driving. Technical Report 23-Nov-2016, 5G Automotive Association, Neumarkter Str. 21 81673, Munich Germany, 2016.

[11] 5G Automotive Association. An assessment of direct communications technologies for improved road safety in the EU. pages 1–80, December 2017.

[12] Ericsson AB. 5G security – enabling a trustworthy 5G system. Ericsson white paper, Ericsson AB, Torshamnsgatan 21, Stockholm, Sweden, March 2018.

[13] T. Aguilera, F. J. Alvarez, A. Sanchez, D. F. Albuquerque, J. M.N. Vieira, and S. I. Lopes. Characterization of the Near-Far problem in a CDMA-based acoustic localization system. *Proceedings of the IEEE International Conference on Industrial Technology*, 2015-June(June):3404–3411, 2015. doi: 10.1109/ICIT.2015.7125604.

[14] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. 5G security: Analysis of threats and solutions. *2017 IEEE Conference on Standards for Communications and Networking, CSCN 2017*, pages 193–199, 2017. doi: 10.1109/CSCN.2017.8088621.

[15] Ala'a Al-Momani, Frank Kargl, Christian Waldschmidt, Steffen Moser, and Frank Slomka. Wireless channel-based message authentication. *IEEE Vehicular Networking Conference, VNC*, pages 271–274, January 2016. ISSN 21579865. doi: 10.1109/VNC.2015.7385587.

[16] A Ali, H Cao, J Eichinger, S Gangakhedkar, and M Gharba. A Testbed for Experimenting 5G-V2X Requiring Ultra Reliability and Low-Latency. *WSA 2017; 21th International ITG Workshop on Smart Antennas*, pages 1–4, 2017.

[17] Bayu Anggorojati and Ramjee Prasad. Securing Communication in Inter Domains Internet of Things using Identity-based Cryptography. *2017 International Workshop on Big Data and Information Security (IWBIS)*, pages 137–142, 2017.

[18] Ghada Arfaoui, Jose Manuel Sanchez Vilchez, and Jean Philippe Wary. Security and resilience in 5G: Current challenges and future directions. *Proceedings - 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 11th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Conference on Embedded Software and Systems*, pages 1010–1015, 2017. doi: 10.1109/Trustcom/BigDataSE/ICESS.2017.345.

[19] J. Arkko and H. Haverinen. Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA). Technical report, The Internet Society, Network Working Group, 2006.

[20] Kaigui Bian, Gaoxiang Zhang, and Lingyang Song. Toward Secure Crowd Sensing in Vehicle-to-Everything Networks. *IEEE Network*, pages 1–6, 2017. ISSN 08908044. doi: 10.1109/MNET.2017.1700098.

[21] Mate Boban, Konstantinos Manolakis, Mohamed Ibrahim, Samer Bazzi, and Wen Xu. Design aspects for 5G V2X physical layer. *2016 IEEE Conference on Standards for Communications and Networking, CSCN 2016*, 2016. doi: 10.1109/CSCN.2016.7785161.

[22] Sherif Adeshina Busari, Kazi Mohammed Saidul Huq, Shahid Mumtaz, Linglong Dai, and Jonathan Rodriguez. Millimeter-Wave Massive MIMO Communication for Future Wireless Systems: A Survey. *IEEE Communications Surveys & Tutorials*, (c), 2017. ISSN 1553-877X. doi: 10.1109/COMST.2017.2787460.

[23] Alin-Mihai Cailean and Mihai Dimian. Towards Environmental-Adaptive Visible Light Communications Receivers for Automotive Applications: A Review. *IEEE Sensors Journal*, 16(c):1–1, 2016. ISSN 1530-437X. doi: 10.1109/JSEN.2016.2529019.

[24] Doru Calin, Harish Viswanathan, Nokia Bell Labs, Mountain Avenue, P O Box, and Murray Hill. Optimal Path Selection in Multi-RAT Wireless Networks. *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications Dynamic*, pages 363–368, 2016.

[25] Ben Jye Chang, Ying Hsin Liang, and Yao De Huang. Efficient Emergency Forwarding to Prevent Message Broadcasting Storm in Mobile Society via Vehicle-to-X Communications for 5G LTE-V. *Proceedings - 2016 International Computer Symposium, ICS 2016*, pages 479–484, 2017. doi: 10.1109/ICS.2016.0102.

[26] Shanzhi Chen, Jinling Hu, Yan Shi, Ying Peng, Jiayi Fang, Rui Zhao, and Li Zhao. Vehicle-to-Everything (v2x) Services Supported by LTE-Based Systems and 5G. *IEEE Communications Standards Magazine*, 1:70–76, 2017. ISSN 2471-2825. doi: 10.1109/MCOMSTD.2017.1700015.

[27] 5GCAR consortium. 5GCAR first report: The 5GCAR EU initiative pushes for future wireless vehicular communication. 2017. URL `https://5gcar.eu/wp-content/uploads/2017/11/First-5GCAR-Press-release_20171017.pdf`.

[28] Martin Dehnel-wild and Cas Cremers. Security vulnerability in 5G-AKA draft. Technical report, Department of Computer Science, University of Oxford, 2018.

[29] Boya Di, Lingyang Song, Yonghui Li, and Geoffrey Ye Li. NOMA-Based Low-Latency and High-Reliable Broadcast Communications for 5G V2X Services. *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, pages 1–6, 2017.

[30] Boya Di, Lingyang Song, Yonghui Li, and Geoffrey Ye Li. Non-Orthogonal Multiple Access for High-Reliable and Low-Latency V2X Communications in 5G Systems. *IEEE Journal on Selected Areas in Communications*, 35:2383–2397, 2017. ISSN 07338716. doi: 10.1109/JSAC.2017.2726018.

[31] Zakarya Drias, Ahmed Serhrouchni, and Olivier Vogel. Identity-Based Cryptography (IBC) Based Key Management System (KMS) for Industrial Control Systems (ICS). *Cyber Security in Networking Conference (CSNet), 2017 1st*, pages 1–10, 2017.

[32] Xiaoyu Duan, Yanan Liu, and Xianbin Wang. SDN enabled 5G-VANET: Adaptive vehicle clustering and beamformed transmission for aggregated traffic. *IEEE Communications Magazine*, 55(7):120–127, 2017. ISSN 01636804. doi: 10.1109/MCOM.2017.1601160.

[33] Ericsson AB. 5G Security-Scenarios and Solutions. Technical report, Ericsson AB, Torshamnsgatan 21, Stockholm, Sweden, June 2017.

[34] Dongfeng Fang, Yi Qian, and Rose Qingyang Hu. Security for 5G Mobile Wireless Networks. *IEEE Access*, pages 1–24, 2017. ISSN 21693536. doi: 10.1109/ACCESS.2017.2779146.

[35] Sadegh Farhang, Yezekael Hayel, and Quanyan Zhu. PHY-layer location privacy-preserving access point selection mechanism in next-generation wireless networks. *2015 IEEE Conference on Communications and NetworkSecurity, CNS 2015*, pages 263–271, 2015. doi: 10.1109/CNS.2015.7346836.

[36] Alessio Filippi, Kees Moerman, Vincent Martinez, Andrew Turley, N X P Semiconductors, Onn Haran, and Ron Toledano Autotalks. IEEE802.11p ahead of LTE-V2V for safety applications. 2017.

[37] 5GPPP Architecture Working Group. 5GPPP Architecture Working Group View on 5G Architecture. Technical Report Jan-2018-v2.0, 5GPPP, Wieblinger Weg 19/4, 69123 Heidelberg, Germany, December 2017.

[38] Mahmoud Hashem Eiza, Qiang Ni, and Qi Shi. Secure and Privacy-Aware Cloud-Assisted Video Reporting Service in 5G-Enabled Vehicular Networks. *IEEE Transactions on Vehicular Technology*, pages 7868–7881, 2016. ISSN 00189545. doi: 10.1109/TVT.2016.2541862.

[39] Huawei Technologies Co. 5G Security: Forward Thinking Huawei White Paper. Technical report, Huawei Technologies Co., Huawei Base, Bantian, Longgang District, Shenzhen, China, 2015.

[40] Huawei Technologies Co. 5G Scenarios and Security Design. Technical report, Huawei Technologies Co., Huawei Base, Bantian, Longgang District, Shenzhen, China, November 2016.

[41] European Telecommunications Standards Institute. Network domain security; authentication framework; (release 6). ETSI Technical Specification Group Service and System Aspects TS 133 310, 3GPP, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, February 2004.

[42] European Telecommunications Standards Institute. 3G Security; Network Domain Security; IP network layer security (Release 9). ETSI Technical Specification Group Service and System Aspects TS 133 210, 3GPP, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2009.

[43] European Telecommunications Standards Institute. Basic Set of Applications; Definitions. ETSI technical report on Vehicular Communications TR 102 638 - V1.1.1, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2009.

[44] European Telecommunications Standards Institute. Part 3 : Specifications of Decentralized Environmental Notification Basic Service. ETSI technical specification on Vehicular Communications TS 102 637-3, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2010.

[45] European Telecommunications Standards Institute. Security Services and Architecture. ETSI technical specification on Intelligent Transport Systems (ITS) TS 102 731, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2010.

[46] European Telecommunications Standards Institute. Communications Architecture. ETSI european standard on Intelligent Transport Systems (ITS) EN 302 665 - V1.1.1, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2010.

[47] European Telecommunications Standards Institute. Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol. ETSI technical specification on Vehicular Communications TS 102 636-5-1 - V1.1.1, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2011.

[48] European Telecommunications Standards Institute. Basic Set of Applications; Part 2 : Specification of Cooperative Awareness Basic Service. ETSI technical specification on Vehicular Communications TS 102 637-2, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2011.

[49] European Telecommunications Standards Institute. ITS communications security architecture and security management. ETSI technical specification on Intelligent Transport Systems (ITS) TS 102 940 - V1.1.1, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2012.

[50] European Telecommunications Standards Institute. Security; Trust and Privacy Management. ETSI technical specification on Intelligent Transport Systems (ITS) 102 941 - V1.1.1, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2012.

[51] European Telecommunications Standards Institute. GeoNetworking. ETSI technical specification on Vehicular Communications TS 102 636-4-1 - V1.1.1, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2013.

[52] European Telecommunications Standards Institute. Security; Security header and certificate formats. ETSI technical specification on Intelligent Transport Systems (ITS) TS 103 097 - V1.1.1, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2013.

[53] European Telecommunications Standards Institute. Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture. ETSI Technical Specification on Digital cellular telecommunications system (Phase 2+) TS 133 401 - V10.3.0, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2013.

[54] European Telecommunications Standards Institute. Proximity-services (ProSe) User Equipment (UE) to ProSe function protocol aspects; Stage 3. ETSI Technical Specification on Universal Mobile Telecommunications System (UMTS);

LTE TS 124 334 - V14.0.0, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2015.

[55] European Telecommunications Standards Institute. Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2. ETSI Technical Specification on LTE TS 136 300 - V11.14.0, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2016.

[56] European Telecommunications Standards Institute. Service requirements for V2X services. ETSI technical specification on LTE TS 122 185 - V14.3.0 Release 14, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2017.

[57] European Telecommunications Standards Institute. Architecture enhancements for V2X services. ETSI Technical Specification on Universal Mobile Telecommunications System (UMTS); LTE TS 123 285 - V14.3.0, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2017.

[58] European Telecommunications Standards Institute. Proximity-based services (ProSe); Stage 2. ETSI Technical Specification on Universal Mobile Telecommunications System (UMTS); LTE TS 123 303 - V14.1.0, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2017.

[59] European Telecommunications Standards Institute. Security aspect for LTE support of Vehicle-to-Everything (V2X) services. ETSI Technical Specification on LTE; 5G TS 133 185 - V14.0.0, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2017.

[60] European Telecommunications Standards Institute. User equipment (ue) to v2x control function; protocol aspects; stage 3. ETSI Technical Specification on LTE TS 124 386 - V14.3.0, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2018.

[61] European Telecommunications Standards Institute. Group Communication System Enablers for LTE (GCSE_LTE); MB2 reference point; Stage 3. ETSI Technical Specification on Universal Mobile Telecommunications System (UMTS); LTE TS 129 468 - V14.3.0, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE, 2018.

[62] Institute of Electrical and Electronics Engineers. Part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements 802.11p-2010, IEEE, 3 Park Avenue, New York, NY 10016-5997, USA.

[63] Institute of Electrical and Electronics Engineers. IEEE Std 1609.3-2010: Networking Services. Technical report, IEEE, 3 Park Avenue New York, NY 10016-5997 USA, December 2010.

[64] Institute of Electrical and Electronics Engineers. Security Services for Applications and Management Messages. IEEE Standard for Wireless Access in Vehicular Environments - Redline 1609.2-2016, IEEE, 3 Park Avenue New York, NY 10016-5997 USA, March 2016.

[65] P. Karthik, B. Muthu Kumar, B. A. Ravikiran, K. Suresh, and Glenson Toney. Implementation of visible light communication (VLC) for vehicles. *Proceedings of 2016 International Conference on Advanced Communication Control and Computing Technologies, ICACCCT 2016*, (978):673–675, 2017. doi: 10.1109/ICACCCT.2016.7831724.

[66] Refik Caglar Kizilirmak. Non-Orthogonal Multiple Access (NOMA) for 5G Networks. In Hossein Khaleghi Bizaki, editor, *Towards 5G Wireless Networks - A Physical Layer Perspective*, chapter 04. InTech, Rijeka, 2016. doi: 10.5772/66048. URL `http://dx.doi.org/10.5772/66048`.

[67] Kjell Larsson, Björn Halvarsson, Damanjit Singh, Ranvir Chana, and Jawad Manssour. High-Speed Beam Tracking Demonstrated Using a 28 GHz 5G Trial System. *Vehicular Technology Conference (VTC-Fall), 2017 IEEE 86th*, 2017.

[68] Ming Liu, Yuming Mao, Supeng Leng, and Sun Mao. Full-Duplex Aided User Virtualization for Mobile Edge Computing in 5G Networks. *IEEE Access*, 2017. ISSN 21693536. doi: 10.1109/ACCESS.2017.2786662.

[69] Petri Luoto, Mehdi Bennis, Pekka Pirinen, Sumudu Samarakoon, Kari Horneman, and Matti Latva-Aho. Vehicle clustering for improving enhanced LTE-V2X network performance. *EuCNC 2017 - European Conference on Networks and Communications*, pages 1–5, 2017. doi: 10.1109/EuCNC.2017.7980735.

[70] Nasser Nowdehi and Tomas Olovsson. Experiences from implementing the ETSI ITS SecuredMessage service. *IEEE Intelligent Vehicles Symposium, Proceedings*, (Iv):1055–1060, 2014. ISSN 1931-0587. doi: 10.1109/IVS.2014.6856587.

[71] Wooguil Pak. Fast packet classification for V2X services in 5G networks. *Journal of Communications and Networks*, (3):218–226, 2017. ISSN 12292370. doi: 10.1109/JCN.2017.000039.

[72] Fei Pan, Hong Wen, Huanhuan Song, Tang Jie, and Longye Wang. 5G Security Architecture and Light Weight Security Authentication. *2015 IEEE/CIC International Conference on Communications in China: First International Workshop on Green and Secure Communications Technology*, 2015.

[73] Wei Peng, Song Liu, Kunlun Peng, Jin Wang, and Jin Liang. A secure publish/subscribe protocol for Internet of Things using identity-based cryptography. pages 628–634, 2017. doi: 10.1109/ICCSNT.2016.8070234.

[74] Qualcomm. Designing 5G NR. Technical Report April, Qualcomm, 2018.

[75] Gandeva Bayu Satrya and Soo Young Shin. Security Enhancement to Successive Interference Cancellation Algorithm for Non-Orthogonal Multiple Access

(NOMA). *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pages 5–9, 2017.

[76] Adi Shamir. IDENTITY-BASED CRYPTOSYSTEMS AND SIGNATURE SCHEMES. *Advances in Cryptology - CRYPT0 '84, LNCS 196*, pages 47–53, 1984.

[77] John N Soliman and Tarek Abdel Mageed. Taxonomy of Security Attacks and Threats in Cognitive Radio Networks. *2017 Japan-Africa Conference on Electronics, Communications and Computers (JAC-ECC)*, pages 127–131, 2017.

[78] Li Sun and Qinghe Du. Physical Layer Security with Its Applications in 5G Networks : A Review. *China Communications*, pages 1–14, 2017.

[79] Kiichi Tateishi, Daisuke Kurita, Atsushi Harada, Yoshihisa Kishiyama, Shoji Itoh, Hideshi Murai, Nicolas Schrammar, Arne Simonsson, and Peter Okvist. Experimental evaluation of advanced beam tracking with CSI acquisition for 5G radio access. *IEEE International Conference on Communications*, 2017. ISSN 15503607. doi: 10.1109/ICC.2017.7996953.

[80] The 5G Infrastructure Public Private Partnership. 5G Automotive Vision. Technical Report 2015, The 5G Infrastructure Public Private Partnership, Wieblinger Weg 19/4, 69123 Heidelberg, Germany, 2015.

[81] Vutha Va, Haris Vikalo, and Robert W. Heath. Beam tracking for mobile millimeter wave communication systems. *2016 IEEE Global Conference on Signal and Information Processing, GlobalSIP 2016 - Proceedings*, (1):743–747, 2017. doi: 10.1109/GlobalSIP.2016.7905941.

[82] Hima Bindu Valiveti. Light Fidelity Handoff Mechanism for Content Streaming in High Speed Rail Networks. *2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pages 488–492, 2017.

[83] Huaxia Wang, Yu-Dong Yao, Xin Zhang, and Hongbin Li. Secondary User Access Control in Cognitive Radio Networks. *IEEE Journal on Selected Areas in Communications*, 34(11):2866–2873, 2016. ISSN 0733-8716. doi: 10.1109/JSAC.2016.2615262.

[84] Pengjin Xie, Jingchao Feng, Zhichao Cao, and Jiliang Wang. GeneWave: Fast authentication and key agreement on commodity mobile devices. *Proceedings - International Conference on Network Protocols, ICNP*, 2017-October, 2017. ISSN 10921648. doi: 10.1109/ICNP.2017.8117543.

[85] Ping Xie, Moli Zhang, Gaoyuan Zhang, Ruijuan Zheng, Ling Xing, and Qingtao Wu. On physical-layer security for primary system in underlay cognitive radio networks. *IET Networks*, 7(2):68–73, 2018. ISSN 2047-4954. doi: 10.1049/iet-net.2017.0138.

[86] Datong Xu, Pinyi Ren, Qinghe Du, Li Sun, and Yichen Wang. Combat eavesdropping by full-duplex technology and signal transformation in non-orthogonal multiple access transmission. *IEEE International Conference on Communications*, (i), 2017. ISSN 15503607. doi: 10.1109/ICC.2017.7997115.

[87] Datong Xu, Pinyi Ren, Qinghe Du, Li Sun, and Yichen Wang. Design for NOMA : Combat Eavesdropping and Improve Spectral Efficiency in the Two-User Relay Network. *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, (61461136001), 2017.

[88] Elias Yaacoub and Mohammed Al-Husseini. Achieving physical layer security with massive MIMO beamforming. *2017 11th European Conference on Antennas and Propagation, EUCAP 2017*, pages 1753–1757, 2017. doi: 10.23919/EuCAP.2017.7928045.

[89] Ruiyun Yu, Zhihong Bai, Leyou Yang, Pengfei Wang, Oguti Ann Move, and Yonghe Liu. A Location Cloaking Algorithm Based on Combinatorial Optimization for Location-Based Services in 5G Networks. *IEEE Access*, 4:6515–6527, 2016. ISSN 21693536. doi: 10.1109/ACCESS.2016.2607766.

[90] Xiaowei Zhang, Andreas Kunz, and Stefan Schroder. Overview of 5G security in 3GPP. *2017 IEEE Conference on Standards for Communications and Networking, CSCN 2017*, pages 181–186, 2017. doi: 10.1109/CSCN.2017.8088619.

[91] Jiaqi Zhao, Mengjie Zhang, Shangyu Liang, Jin Ding, Fumin Wang, Xingyu Lu, Can Wang, and Nan Chi. 100-m field trial for 5G wireless backhaul based on circular (7,1) 8-QAM modulated outdoor visible light communication. *2017 Opto-Electronics and Communications Conference (OECC) and Photonics Global Conference (PGC)*, pages 1–4, 2017. doi: 10.1109/OECC.2017.8114757.

[92] Shuangrui Zhao, Jia Liu, Xiaochen Li, and Student Member. Secure Beamforming for Full-duplex MIMO Two-way Communication via Untrusted Relaying. *2017 IEEE Globecom Workshops (GC Wkshps)*, 2017.

[93] Chan Zhou and Wolfgang Kellerer. Multi-User-Centric Virtual Cell Operation for V2X Communications in 5G Networks. *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 84–90, 2017.

[94] Yao Zou, Chen Tang, Varun Jain, and Stephan Lapoehn. 5G Enabled Cooperative Collision Avoidance : System Design and Field Test. *A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2017.