5G for automated and connected cars

Markku Leppälä

School of Electrical Engineering

Bachelor's thesis
Espoo 01.09.2019

Supervisor

PhD Samuli Aalto

Advisor

Dr Giancarlo Pastor Figueroa

Aalto University
School of Electrical
Engineering

Aalto University
School of Electrical
Engineering

Aalto University, P.O. BOX 11000, 00076 AALTO
www.aalto.fi
Abstract of the bachelor's thesis

Author Markku Leppälä

Title 5G for automated and connected cars

Degree programme Electronics and electrical engineering

Major Information Technology **Code of major** ELEC3015

Teacher in charge PhD Samuli Aalto

Advisor Dr Giancarlo Pastor Figueroa

Date 01.09.2019 **Number of pages** 27 **Language** English

Abstract

5G protocol is about to be released out for consumer use later in 2020. The protocol offers new possibilities for mobile data services in multiple sectors of industry. Regardless of technical advancing of the 5G protocol it still has pressing security challenges besides the growing concerns for user privacy.

Meanwhile, the first iterations of automated and connected cars are rolling out to public roads amidst the human steered cars. Automated cars require high broadband connectivity in order to communicate with other cars and supporting infrastructure. This Bachelor's thesis examines the possibilities 5G networks offer for automated and connected cars. The thesis also compares the requirements automated and connected cars have for data integrity, security, and privacy on transmission channel focusing on possible security challenges. The research is accomplished as a literature review based on the latest research articles in the field.

Keywords 5G, 5G security, automated car, connected car

Aalto University
School of Electrical
Engineering

Aalto-yliopisto, PL 11000, 00076 AALTO
www.aalto.fi
Tekniikan kandidaatintyön tiivistelmä

Tekijä Markku Leppälä

Työn nimi 5G itseohjautuville ja yhdistetyille autoille

Koulutusohjelma Elektroniikka ja sähkötekniikka

Pääaine Informaatioteknologia **Pääaineen koodi** ELEC3015

Vastuuopettaja TkT Samuli Aalto

Työn ohjaaja TkT Giancarlo Pastor Figueroa

Päivämäärä 01.09.2019 **Sivumäärä** 27 **Kieli** Englanti

Tiivistelmä

Uusin mobiiliverkkoteknologia, 5G, tullaan ottamaan laajasti käyttöön vuonna 2020. 5G-teknologia tarjoaa ennennäkemättömän teknisen suorituskyvyn niin tiedostonsiirron nopeuden kuin viiveajan puolesta. Tämän teknologian avulla tullaan toteuttamaan useita uudenlaisia sovelluksia, kuten älykkäitä kaupunkeja sekä autonomisia ja keskenään kommunikoivia autoja. Samaan aikaan globaalit kyberuhat kasvavat ja rikolliset uhkaavat julkisia palveluita, kuten sairaaloita ja pankkeja. On elintärkeää varmistaa uusien teknologioiden tietoturvallisuus ennen laajamittaista käyttöönottoa.

Tässä kandidaatintyössä tarkastellaan yleisesti 5G-protokollan uusia teknologioita sekä näiden tarjoamia mahdollisuuksia autonomisille ja yhdistetyille autoille. Vastaavasti käydään läpi autonomisten autojen toimintaa ja vaatimuksia, joita verrataan 5G-mobiiliverkon oletettuun suorituskykyyn selvittääkseen mahdolliset puutteet. 5G-verkon luotettavuutta tietoturvallisuuden sekä yksityisyydensuojan osalta tarkastellaan erityisen tarkasti. Kandidaatintyö toteutetaan kirjallisuuskatsauksena, ilman empiiristä tutkimusta. 5G protokollaa kehitetään jatkuvasti eteenpäin, joten työssä tutkitaan 5G:n ydinteknologioita sekä alan viimeisimpiä tutkimuksia.

Työssä verrataan 5G-mobiiliverkon määriteltyä suorituskykyä useilla eri parametreilla, kuten tiedostonsiirtonopeuden, viiveajan, kattavuuden sekä käytössäoloajan osalta itseohjautuvien autojen vaatimuksiin. Kandidaatintyössä havaitaan, että 5G-standardissa määriteltyjen suorituskykyparametrien toteutuessa nämä riittäisivät palvelemaan nykymuotoisia autonomisia ja keskenään kommunikoivia autoja. Tutkielmassa tarkastellaan nykyisen 5G-standardin tietoturvallisuuden tasoa, yksityisyydensuojaa sekä mahdollisia muita puutteita. Autonomisilla autoilla on korkeat vaatimukset tietoturvan osalta, sillä mahdolliset haavoittuvuudet saattavat uhata ihmishenkiä sekä aiheuttaa laajoja rahallisia haittoja. Työssä huomataan, että osassa teknologioista, kuten käyttäjän todentamisessa on nykyisellä toteutuksella puutteita. 5G-protokollaan on ehdotettu 5G-AKA-todentaminen, joka mahdollistaa viestien uudelleentoistohyökkäykset, joilla voidaan paikantaa käyttäjän sijainti verkon sisällä. Tämä todentamisteknologia on puutteellinen, ja uhkaa käyttäjän yksityisyyttä. Puutteet käyttäjän todentamisessa voivat mahdollistaa myös verkon resurssien käyttämisen niin, että laskutus kohdistuu toiselle käyttäjälle. Tarkastelun kohteena on myöskin verkon arkkitehtuuriset ratkaisut. 5G-protokolla mahdollistaa käyttäjien tai palveluiden hyödyntävän verkon tukiasemissa sijaitsevia laskenta- tai tallennusresursseja. Näitä resursseja voidaan hyödyntää autonomisten autojen sovelluksissa, kuten anturi- tai kameradatan analysoinnissa. Uudenlainen teknologia mahdollistaa lasken-

tatehollisesti vaativien sovellusten toteuttamisen erittäin pienellä latenssilla, mikä on elinehtona itseohjautuvien autojen nopealle reagointikyvylle. Uudenlaiset verkon arkkitehtuuriset ratkaisut kuitenkin mahdollistavat hyökkäysrajapintoja, jotka tulee tutkia tarkoin ennen sovellusten käyttöönottoa.

Tutkielmassa tarkastellaan 5G-verkon mahdollisuuksia autonomisille ja yhdistetyille autoille sekä tutkitaan mahdollisia tietoturvallisuushaasteita. 5G mobiiliverkko on aiempia mobiiliverkkoteknologioita huomattavasti suorituskykyisempi, mikä riittää palvelemaan itseohjautuvien ja yhdistettyjen autojen nykyisiä tarpeita. 5G-verkko tullaan ottamaan laajasti käyttöön vuonna 2020, joten teknologia on vielä jatkuvassa kehityksessä. Nykyisestä 5G:n toteutusmallista löydetään heikkouksia, jotka mahdollistavat muun muassa erilaisia hyökkäysrajapintoja, jotka voivat esimerkiksi vahingoittavat käyttäjän yksityisyyttä. 5G-verkon arkkitehtuurisista sekä teknologisista ratkaisusta johtuen muodostuu uudenlaisista rajapintoja, jotka täytyy tutkia tarkoin ennen kriittisten teknologioiden laajamittaista käyttöönottoa.

Avainsanat 5G, 5G-tietoturva, itseohjautuva auto, yhdistetty auto

Contents

Abbreviations

3GPP	The Third Generation Partnership Project
5G	Fifth-generation
ACC	Adaptive Cruise Control
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
C-V2X	Cellular-Vehicle to Everything
CC	Critical Communications
CUPS	Control-user plane separation
DDoS	Distributed Denial-of-Service
eMMB	Enhanced Mobile Broadband
E-UTRAN	Evolved UMTS Radio Access Network
EPC	Evolved Packet Core
Gbps	Gigabytes per second
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HN	Home Network
IMT	International Mobile Telecommunications
IoT	Internet of Things
ITU	International Telecommunication Union
KPI	Key Performance Indicator
LIDAR	Light Detection and Ranging
LTE	Long-Term Evolution
Mbps	Megabytes per second
MEC	Multi-Access Edge Computing
MMTC	Massive Machine Type Communications
MNO	Mobile Network Operator
NFV	Network Function Virtualization
NR	New Radio
NSSF	Network Slice Selection Function
NSA	Non-Stand Alone
RADAR	Radio Detection and Ranging
RSU	Road Side Unit
SA	Stand-Alone
SAE	Society of Automotive Engineers
SMF	Session Management Function
SN	Serving Network
UE	User Equipment
UPF	User Plane Function
URLLC	Ultra-Reliable and Low Latency Communication
USIM	Universal Subscriber Identity Module
V2I	Vehicle-to-infrastructure
V2X	Vehicle-to-everything
VNF	Virtual Network Functions

1 Introduction

The fifth-generation (5G) network is the latest generation of cellular mobile communications. Performance-wise, it is designed to achieve high data rate, reduced latency, high adjustability, energy savings, high capacity, and support for industries via massive device connectivity often called Internet of Things (IoT). These increased performance and novel technologies introduced by the 5G standard offer new possibilities for multiple industries and applications such as factories and automated cars [1]. However, harnessing premature technologies without extensive research is exposing devices for external attacks and risking lives in critical applications such as automotive and transportation. Thus it is crucial to investigate the technologies used in the later phases of the development.

Apart from the increased speed and low communication latency, one significant advantage in the protocol is the possibility of network slicing. 5G systems are to be built in a way enabling logical network slices, which can be modified to allow telecom operators to provide a network on an as-a-service basis. These slices can be highly modified based on the needs of customers to meet a wide range of use cases. Network slicing technology can provide connectivity for emergency services requiring high availability and low latency. At the same time, another network slice offers high throughput connectivity for streaming in a car on the move. A single 5G system can serve multiple slices simultaneously for a single device. [1]

While the development of the 5G protocol is reaching closer towards the production version, automated and connected cars are becoming more popular. Automated cars are observing the environment via multiple inputs such as high-resolution cameras and optical radars, meanwhile producing an extensive amount of data. The recent progress in real-time computing is already enabling powerful algorithms to take control of cars to execute simple tasks such as steering, adaptive cruise control (ACC), and parking [2].

The network of fully automated and connected cars require low latency and high availability of mobile network connections to enable co-operation between the cars and infrastructure. The performance and functional properties of the network slices can be modified optimally with network slicing, to meet these requirements. These new 5G technologies, however, have pressing security challenges to secure data integrity and privacy in critical communications [3] requiring extensive research before implementing these technologies into use.

This Bachelor's thesis examines the new possibilities 5G networks offer for automated and connected cars. The main question to answer is will the 5G technology offers sufficient performance for fully automated and connected vehicles. This thesis also examines what challenges does the 5G platform face and does it offer sufficient privacy and security for automated and connected cars. This thesis is a literature review with no empirical research. The first chapter examines the technological solutions of the 5G standard and provided new features. The second chapter compares the preconditions that automated and connected cars pose for a network. The third chapter maps possible security challenges automated and connected cars face at mobile network communication and present ways to secure the connection.

2 5G protocol

The 5G protocol has been predicted as a significant enable for multiple verticals such as smart cities or automotive. The 5G cellular mobile communication network is about to be harnessed into use in 2020 [4]. 5G is the newest version of the evolutionary process, in which earlier versions have been named accordingly as anterior generations. The latest generation will inherit technologies from the predecessors, but also bring in new features. The most notable changes are significant improvements in performance and the possibility for different network profiles supporting various use cases for different industries such as automotive.

The specifications are defined by the 3rd Generation Partnership Project (3GPP), and the 5G standard will be deployed in two phases. One phase consists of multiple stages shown in Figure 1. The first phase, specified in Release 15, addresses the most critical requirements needed for commercial deployment and forms the basis for the first deployment. The second phase, described in Release 16 that is to be completed by the end of 2019 or early 2020. This release will address all remaining requirements, such as support for services including network slicing and Cellular-Vehicle to Everything (C-V2X). The finalization of the second phase will bring new devices to the market that rely on the 5G technologies. These devices include multiple automated car related necessary devices such as on-board units (OBUs). [5]

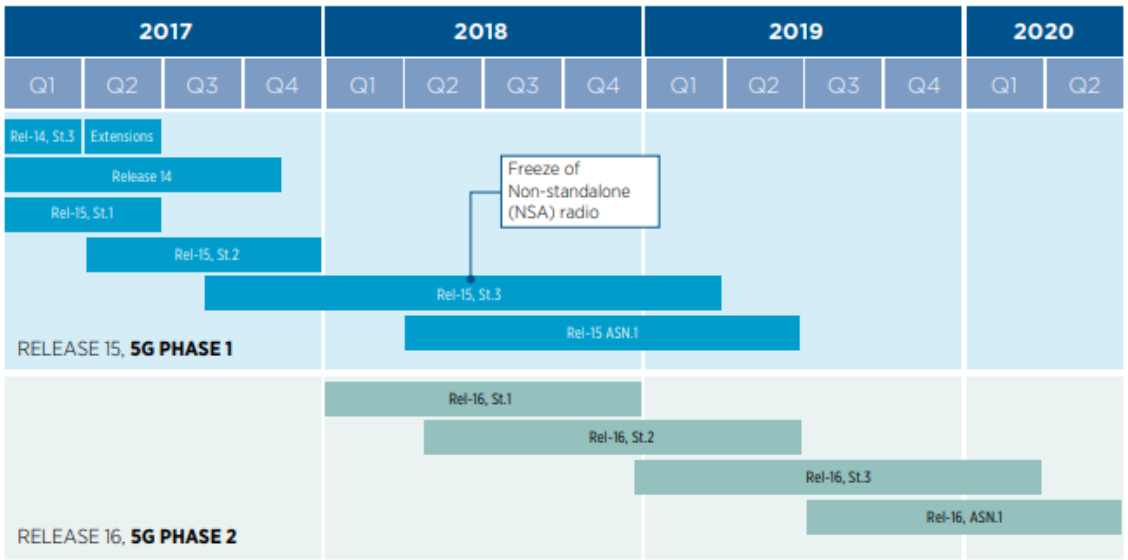

Figure 1: 3GPP roadmap for Release 15 and 16 [6]

The 5G platform will add significant improvements in flexibility for mobile networks by introducing software-defined networking that enables programmatically configuring the network to optimize it for various use-cases. For example, a single 5G system can provide multiple tailored network profiles for different needs, such as events with a massive amount of participants and simultaneously supporting mission-critical emergency service communication [7]. The estimated timeline of the

5G features is illustrated in Figure 2.

As the flexibility and performance of the mobile communication network grow, and the price of the 5G hardware decreases, an increased share of factories are replacing their internal Wi-Fi and Ethernet-based networks with connectivity to private 5G networks [8, 9]. Using 5G will increase the security compared to Wi-Fi networks that have shown to be vulnerable [10] and free the robots from cabling required by fixed ethernet connections. However, migrating away from Wi-Fi networks to private 5G networks requires enterprises to set up their extensive security implementations before taking a new transmission channel into use.

Extensive safety procedures are also required from the 5G technology itself as well as the infrastructure providers, such as mobile network operators (MNO), to ensure safety in mission-critical operations and factories.

The adoption of the 5G technology is expected to be rapid due to the added performance benefits and government level prioritization. Governments around the world have prioritized the development of holistic strategies, underpinned by clear, predictable, and forward-looking regulatory frameworks, to support digital innovation and to facilitate 5G technologies [4].

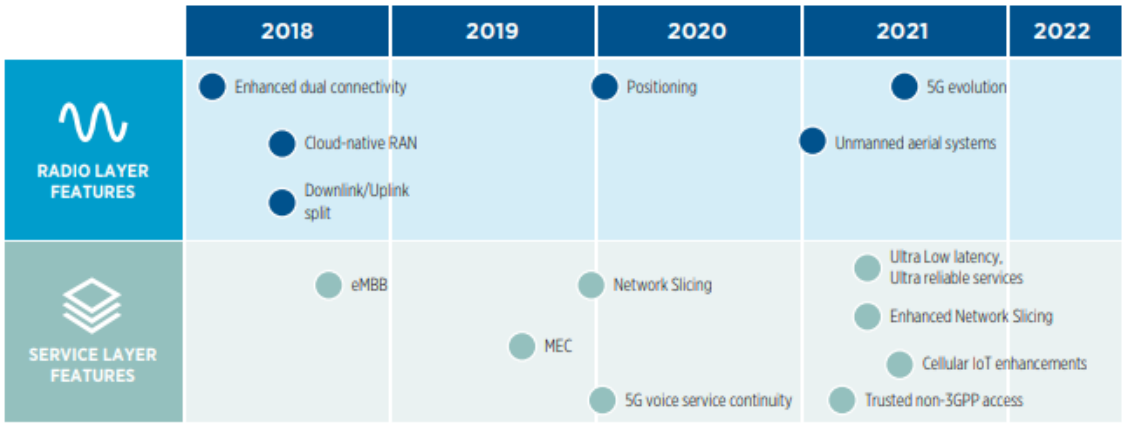

Figure 2: 5G features timeline [6]

2.1 5G architecture

Digitalization creates tremendous opportunities for mobile communication but poses strict challenges towards mobile communication technologies. Diversified demands of future applications require new solutions in the core architecture of 5G. The architecture of 5G has been restructured to meet the demands and offer more flexible solutions. 5G protocol introduces multiple new architectural changes such as control-user plane separation and deployment of Non-Stand Alone architecture to add the flexibility and help the transition toward the Stand-Alone deployment.

2.1.1 Control-user plane separation

The introduction of the control-user plane separation (CUPS) is an essential addition to a 5G core architecture. CUPS increases the flexibility of the 5G technology due to its ability to distribute user plane resources across the network with existing 4G Evolved Packet Core (EPC). The control plane can sit in a centralized location, for example, in the middle of the country, and for the user-plane to be placed closer to the application its supporting [11]. CUPS allows operators to locate and scale the control plane and user plane resources of the EPC nodes independently. Due to the core user plane location closer to the end-user, operators do not have to backhaul traffic all the way to the central data center. Therefore, they can reduce latency, which is crucial for applications such as connected cars. This scenario also supports high-bandwidth applications such as video streams meanwhile reducing the backhaul traffic costs [12].

2.1.2 Non-Stand Alone and Stand-Alone architectures

The 5G network can be deployed in two different ways, with Non-Stand Alone (NSA) and Stand-Alone (SA) architectures. In NSA architecture, the 5G Radio Access Network, also called New Radio (NR) is used in conjunction with the existing Long-Term Evolution (LTE) and 4G infrastructure [13]. Using the existing technologies underneath makes the new 5G-based radio technology available without physical network replacement. This configuration supports only the 4G services, but extended performance capacities of the 5G technology such as ultra-low latency and high throughput are offered. The NSA architecture can be seen as a temporary step forwards the full 5G deployment. The NSA architecture is illustrated in Figure 3, where 5G NR base station (en-gNB) connects to the LTE base station (eNB) to form Evolved UMTS Radio Access Network (E-UTRAN). EPC is formed from Mobile Management Entity (MME) and Serving Gateway (S-GW). MME is the key control-node for the LTE access-network handling User Equipment (UE) tagging and paging procedure, including retransmissions. S-GW mainly routes and forwards user data packets.

The SA 5G architecture is composed of UE, Next-Generation Radio Access Network (NG-RAN) and 5G Core (5GC). In SA architecture, the NR is connected to the 5G Core Network, thus it is fulfilling all the technical specifications and services defined in the 5G Phase 1, as specified in [14]. The SA architecture is illustrated in Figure 4. The approach enables a virtualized deployment. Network Function instance can be deployed as fully distributed, fully redundant, stateless, and fully scalable [13]. 5G is designed to support diverse services with different data traffic profiles, for example, high throughput, low latency, and massive connections. 5G networks are capable of serving one UE with multiple profiles simultaneously through network slicing and hosting services locally particularly through the Edge Computing capability. The new 5G data profiles and services are described in the next section.

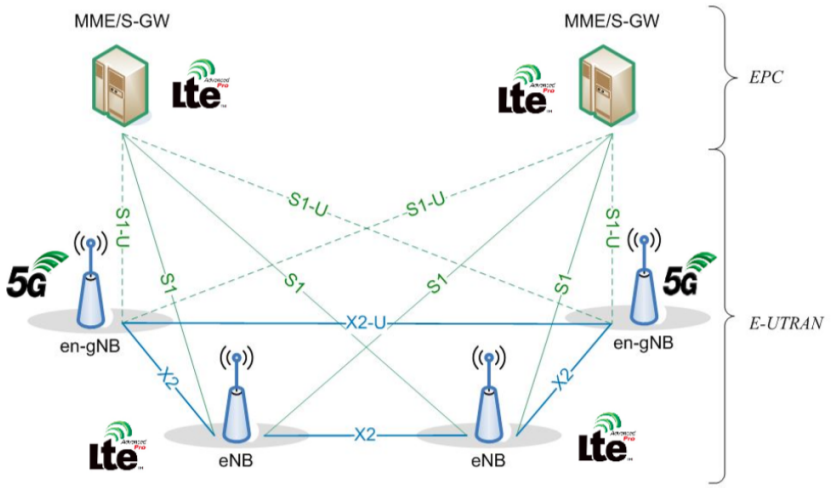

Figure 3: Non-Stand Alone architecture [13]

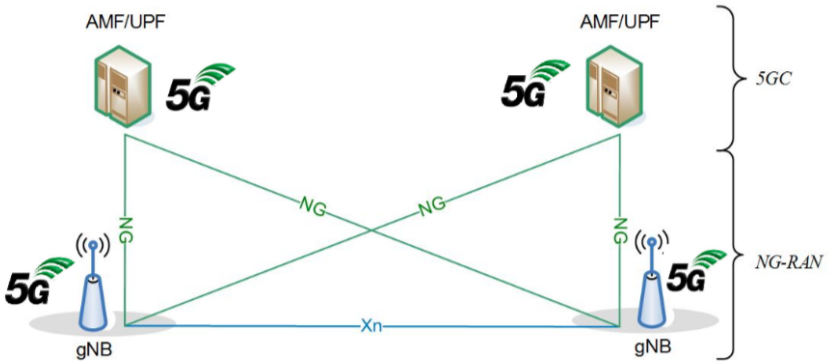

Figure 4: Stand-Alone architecture [13]

2.1.3 Private 5G network

Before the public launch of 5G operators and application providers are willing to test the network and applications such as automated cars in a real environment. The 5G network can be deployed as a private network. A private 5G network is a local area (LAN) network that uses 5G technologies to create a dedicated network. The network is controlled by the owner with independent management. This deployment gains multiple benefits to companies who are looking to replace their internal Wi-Fi networks or usage of public cellular networks with a more flexible option. The private network is flexible as it can be modified to meet the needs of end-user or devices using the network.

The operator of the private network can set up its security policies rather than relying on the outside provider [15] or 5G-AKA authentication discussed in subsection 5.1. For example, safety applications could require more frequent authentication or a multi-layer protocol to verify the data integrity that public cellular networks are not able to provide. The priority of slice can set to allow more resources for high

priority services that are requiring constant availability, low latency and high data throughput.

Private 5G networks are facing some challenges before these can be fully implemented into use. Firstly, the spectrums for 5G networks are currently handled by the MNO's [15], thus setting up a private network might require a hefty investment. Secondly, the deployment of the networks requires technical expertise. A misconfiguration in the settings could grant external attacks full access to the network.

3 5G data profiles and services

Automated and connected cars have multiple very divergent requirements for the network simultaneously. In 5G, the mobile communication network can be split into multiple different data profiles. Each profile has specific performance characteristics based on the use case and the requirements these services have for the network. Three main profiles with extremely different features in performance include Enhanced Mobile Broadband (eMBB), Massive Machine Type Communications (MMTC) and Ultra-Reliable and Low Latency Communication (URLLC) presented in Figure 5. These profiles optimize the available resources for different attributes, including traffic capacity, reliability, latency, connection density, coverage, mobility, and energy consumption. 5G's flexibility enables its use across many verticals such as smart cities, public safety, electricity distribution, media & entertainment, and automotive. [13]

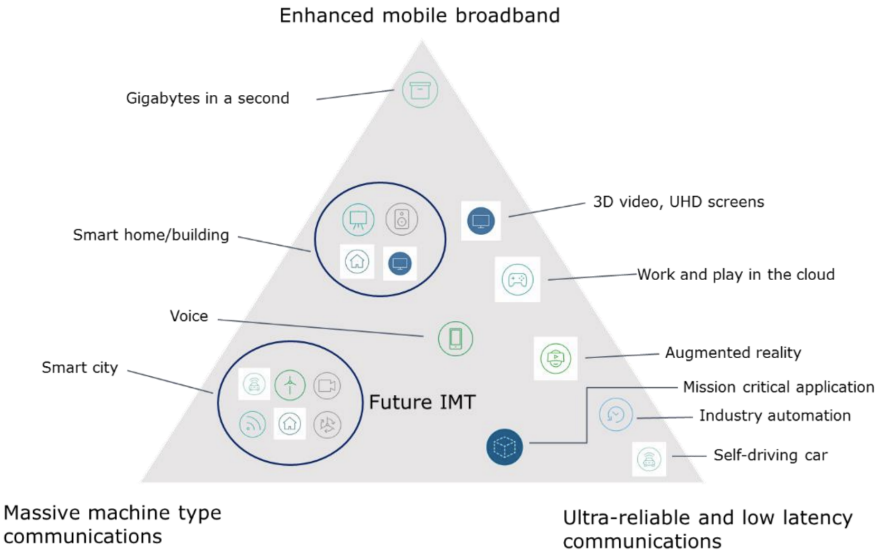

Figure 5: International Telecommunication Union (ITU) 5G services hierarchy [4]

3.0.1 Key performance indicators for network

Automated and connected vehicles have various requirements for the network. The network performance can be evaluated with key performance indicators (KPIs). Table 1 lists the KPIs for common automated driving functions such as advanced driving, vehicle platooning, extended sensors, and remote driving.

- **Payload** is the part of transmitted data that is the actual intended message. Headers and metadata are removed from the size of a transmitted data packet.
- **Tx rate** refers to the number of messages transferred from an automated car towards the network.

- **Max end-to-end latency** is the maximum time allowed for the transportation process, including creating a command, transporting it across the network to the receiver, and transporting back the acknowledgment of successful delivery.
- **Reliability** refers to the service level in the percentage of successful packet transmission expected from the network.
- **Data rate** is the data transmission throughput in the network. Uplink refers to the outbound transmission from the car and the in downlink to the inbound transmission received by the automated car.
- **Minimum required communication range** is the required radius for transmitted messages to travel.

3.0.2 5G use cases for automotive

5G enables multiple use cases for automated driving and connected vehicles. The requirements for each function are different due to the reliability of other devices or distance to the other parties such as RSUs. Table 1 lists some common use cases and network requirements for automotive mentioned in 5G-MOBIX Deliverable 2.1 [16].

Use case	Payload (bytes)	Tx rate (messages/sec)	Max end-to-end latency (ms)	Reliablility (%)	Data rate (Mbps)	Min required communication range (meters)
Advanced Driving	2000-12000	10-100	10-100	90-99.99	10-50	360-700
Vehicle Platooning	50-6000	2-50	10-500	90-99.99	50-65	80-350
Extended Sensors	1600	10	3-100	90-99.999	10-1000	50-1000
Remote Driving	-	-	5	99.999	Uplink: 25 Downlink: 1	-

Table 1: KPIs for automated driving functions [16]

Advanced Driving enables semi-automated or fully-automated driving with longer inter-vehicle distance assumed. Each vehicle or Road Side Unit (RSU) shares data obtained from its local sensors with vehicles in proximity. The shared data allows cars to coordinate their trajectories or maneuvres to avoid collisions and improve traffic efficiency [16]. Due to real-time sensor data is being transmitted the payload size and tx rate is higher than in the other services.

Vehicle Platooning enables vehicles to form a group traveling together dynamically. All the vehicles in the platoon receive periodic data from the leading vehicle to inform the speed or applied braking. This information allows for the distance between cars

to become extremely small, close to sub-second distance [16]. Vehicle platooning requires stable data rates of 50-65 Mbps with a short communication range as the communication happens between cars in the platoon instead of RSUs.

Extended Sensors enable the exchange of raw or processed data gathered by local sensors or live video data among cars, RSUs, devices of pedestrians, and V2X application servers. The cars can enhance the perception of their environment beyond what their own sensors can detect and have a more holistic view of the local environment [16]. Transmitting extensive sensor or video data requires high data rates, up to 1 Gbps. The required communication range can extend up to 1 km to cover the more rural use cases and vehicles such as bullet trains traveling at high speed.

Remote Driving enables the remote driver or a V2X application to operate a remote vehicle. The vehicle can locate in a dangerous environment such as in mining facilities, or the passenger cannot drive themselves. The communication scenario involves an information exchange between user equipment supporting the V2X application and a V2X application server [16]. Remote Driving requires ultra-low, sub 5 ms end-to-end latency, to maximize the car's reaction time. Also, very high reliability, over 99.999%, is required to minimize downtime in a highly sensitive system.

3.0.3 Enhanced Mobile Broadband

eMBB aims to provide high data rates, connection density, and user mobility in various service coverage scenarios. These scenarios include indoor and outdoor areas such as offices, homes, highways, and parks in both rural and urban environments. eMBB can cover special scenarios such as massive gatherings, augmented reality (AR) or virtual reality (VR) media and high-speed cars. Massive gatherings require high unit density and traffic capacity to serve thousands of users with a high-speed connection. AR and VR media require high-speed with low latency to serve users with close to the real-time experience. High-velocity cars such as trains and airplanes require high mobility on top of high transmission speed [14]. [13]

In urban macro scenarios with user density up to 10 000 users/km^2, eMBB is expected to offer up to 50 Mbps download rates. The same download speed can also be achieved in a high-speed train traveling up to 500 km/h. Indoor hotspots are theoretically capable of serving users 1 Gigabyte per second (Gbps) download rates with users up to 250 000 units/km^2 [14]. High data rates on multiple different circumstances can replace Wi-Fi hotspots currently used in public areas and homes, thus improving the security by replacement of unencrypted connections with encrypted ones.

3.0.4 Ultra-Reliable and Low Latency Communication

URLLC and Critical Communications (CC) profiles support the scenarios requiring ultra-low latency and very high communications service availability. The requirements are highly demanded by new technologies such as automated cars, remote surgery, and industrial automation. Often these services require sub 1 ms latency for one

direction transmission and over 99.9999% availability with 10 Mbps data rates and connection density around between 1000 and 100 000 units/km^2. Payloads can range from small to big. [13, 14]

3.0.5 Massive Machine Type Communications

Massive Machine-Type Communications often called Massive IoT, is designed for industrial environments and future smart city applications [4]. Common devices are sensors monitoring attributes such as temperature, acceleration, and ambient light [17] or industrial ones such as printers and packaging machines. A typical characteristic of the communication is small payloads with relatively long time duration between the packets to preserve the energy consumption of the battery-powered sensors. MMTC allows relatively high latency, around 100 ms and a common requirement for availability is ranging from 99.99% to 99.9999%. MMTC has an essential prerequisite for connectivity as it requires a vast amount of sensors being connected to the same network simultaneously. The total number of devices can exceed 10 000 units/km^2. [18]

3.1 Virtual Network Function

Network consists of a large number of intermediate network functions such as load balancer, firewall, and IPsec packet encrypter [19]. Traditionally, these functions have been implemented on special-purpose physical hardware. These platforms are expensive and difficult to maintain and upgrade. Typically network flows go through several network functions, thus deployments easily require varying setups, making it challenging to have a cost-efficient solution for all situations.

Virtual Network Functions (VNF) have been introduced to add flexibility to network implementations. VNFs are software-based functions that can modify the data streams in the same way as the physical hardware. The network functions can be chained to achieve the wanted outcome. For example, Deep Packet Inspector can split the incoming flows over different branches according to the type of the inspected packets. Each of these branches has a fraction of the incoming data flow. Some of the packets can be discarded, thus reducing the data rate in the branches. VNFs able to allocate resources according to the data flow in the branches, thus reducing in lower latency in the throughput.

3.2 Network slicing

Network slicing is a specific form of virtualization, allowing one or multiple logical networks to run on top of a shared physical network infrastructure simultaneously. The 5G protocol architecture splits into different slices described in Figure 6. The logical networks, network slices, are end-to-end connections; thus, the traffic is separated and processed apart from the other traffic. The network slice can serve a network profile with specific services described in the previous chapter, such as an industrial automation profile. The physical network infrastructure can set priorities

for different slices. For example, prioritizing critical and emergency services over eMBB slice. Some network slices can have restrictions on serving only specific types of users; thus, public safety slice can be set to require credentials before traffic transmission. Requiring credentials can improve the security of slices used, which is crucial for CC slices. The Network Slice Selection Function (NSSF) selects the appropriate slice for the end-user and handles the initial connections to the slices. The users can connect to multiple network slices from one device; thus, sophisticated devices can simultaneously connect to different services located in different networks. [13]

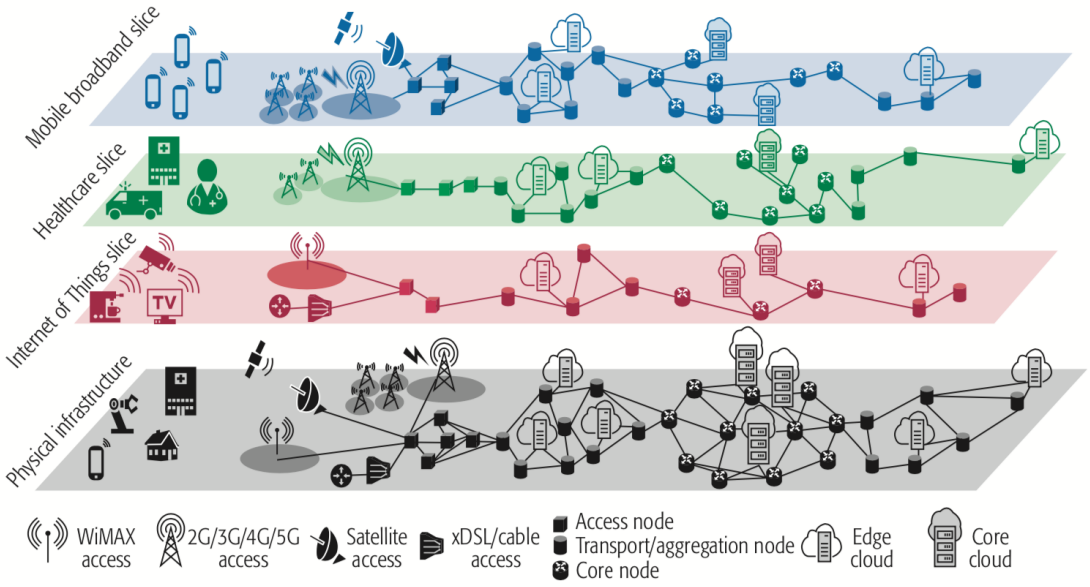

Figure 6: 5G Network Slicing [20]

3.3 Multi-access edge computing

The network slices can also use the physical network infrastructure for storage and computing. These functions are called multi-access edge computing (MEC) that support services requiring high performance by bringing the computing and storage resources closer to the end-user devices. For example, URLLC demands the use of MEC to achieve ultra-low latency requirements. In MEC, the storage and computing resources can be used to process and store data locally, close to the end-user, thus reducing the need for extensive data forwarding all the way to centralized servers. Apart from the latency reductions, the distributed network increases reliability in the network as it is cutting the need for a centralized server. MEC technology is designed to be implemented at the cellular base station or other edge nodes, at the user plane. The applications hosted at the edge can be managed by an operator or a third-party.

MEC is a key enabler for automated cars. The low latency and high reliability offered are highly demanded by traffic safety functions for cars traveling at high

speed. The resources available at the edge are used, for example, to process the data from sensors such as cameras and LIDAR. The data sensors are discussed more in section 4. MEC is estimated to be usable by the end of 2019 [6]; thus it could pave the path for automated and connected cars already in the LTE environment. Using MEC in automated driving could help to increase road safety, optimize infrastructure investment, increase traffic efficiency and comfort, and deliver value-added services [21].

4 Automated and connected cars

Automated cars are fast becoming a reality. Based on estimates, up to 15% of cars will be fully automated, SAE levels 4 and 5 discussed in subsection 4.2, by 2030 [22]. China has even set a target of full autonomy for 10 percent of all automobiles on the road by 2030 [23]. Increased driving assistance and safety mechanisms are automating basic driving tasks and removing human judgment and interaction from the control of the car. Automated and connected cars are massive potential for all cities to increase transportation efficiency and safety for drivers and pedestrians. Over the last two years, the first automated cars have been tested in various countries that allow automated cars such as Australia, the United States of America, and Finland [4, 24]. For example, a level 4 self-driving electric car Sensible 4 has been tested out in Finland in one of the most challenging driving conditions [25, 26, 27]. Sensible 4 is connected to a private 5G test network maintained by Telia and Nokia. The mobile data connection is used to monitor the car and forward the data from the car to the operator.

Before automated and connected cars can be launched for general use, these need approval from the local authorities such as governments. In the European Union framework, multiple projects, such as 5G-MOBIX [28], 5G-CARMEN [29], and 5GCroCo [30] have been launched to coordinate and help the adoption. These projects are aiming to specify, develop, trial, and demonstrate future automotive use cases that require seamless availability of 5G telecommunication features at operator and country borders. Shifting from a country to other requires multiple changes such as adjusting to the driving laws or rules and change of teleoperator that needs to be prepared for.

The majority of the automated car pilots have focused on transportation in different environments amongst regular human-controlled traffic, and some even in varying conditions such as snow and slush [25]. Apart from human transportation, driverless cars such as trucks have been successfully used to transport ores in mines [31]. Using driverless solutions in challenging and even dangerous environments such as mines increase safety for workers who no longer have to undertake dangerous jobs. Based on the estimations, each truck can save around 500 work hours per year. [4]

The key enablers for the fast development of technology and change in the market have been the sophisticated sensors, antennas, and data connectivity technologies in addition to the ever-increasing performance of onboard computing power. Portable computers, together with various inputs such as cameras, sensors, radars, and Global Positioning System (GPS) have increased the sensing and navigation capabilities of automated cars. These capabilities have enabled automated cars to navigate and act upon the external events amongst the traffic in busy cities with various weather scenarios.

Figure 7 demonstrates the multiple sensors, cameras, and safety mechanisms capturing the environment and reacting to the events occurring.

Figure 7: Sensors, cameras, and safety mechanisms of RAC Intellicar [32]

- **3D Light Detection and Ranging (LIDAR)** uses optical lasers giving a 360° peripheral vision. Multiple 3D LIDARs are used to create a 3D map of the environment and detect obstacles in the long-range.
- **Radio Detection and Ranging (RADAR)** determines the position and speed of nearby obstacles.
- **Cameras** are used to analyze road infrastructure and to detect obstacles.
- **Global Navigation Satellite System (GNSS)** uses a constellation of satellites to know the precise location of the car geographically.
- **Odometry** uses motion sensors to estimate its position relative to its starting location.
- **Onboard unit** allows interconnection with urban infrastructure, mostly traffic lights, emergency services, and other cars.
- **Automated emergency braking** applies the brakes automatically if the car senses objects in its path. [32]

A various set of sensors and cameras are needed to cope with different weather situations and add robustness to the data accuracy. A single attribute, such as speed or location needs to be confirmed by multiple sensor inputs. As an example, odometry, the tracking of speed based on wheel rotation is not accurate when wheels are spinning on slippery ice, but the vehicle is not moving. Autonomous and connected cars can be equipped with multiple other sensors and communication equipment, such as short-range radio-based communication helping to communicate with other cars and surrounding infrastructure.

4.1 Connected cars

Connected cars are an integral part of future smart cities. With the help of short-range radio-based exchange or the cellular network connected cars are communicating with other entities. This is called as Vehicle-to-everything (V2X), where infrastructure entities such as traffic lights, lamp posts, highway tolls are connected to the surrounding cars and pedestrians. The V2X messages are broadcasted ten times per second from the car and can include positional data like velocity, angle of steering, location, and amount of throttle or brake applied. V2X communication incorporates other, more specific types of communication illustrated in Figure 8 and listed below.

- Vehicle-to-device (V2D) communication consists of the exchange of information between a vehicle and any electronic device that is connected to the vehicle. For example, a cellphone working to replace car keys or a car-sharing platform are these kinds of devices.
- Vehicle-to-grid (V2G) describes a system in which electric vehicles, such as electric cars, communicate with the power grid to sell energy stored in the vehicle or buy energy to charge the batteries. As most of the cars are used only for a limited time, these parked cars could serve a part in the electric distribution network by regulating energy availability.
- Vehicle-to-infrastructure (V2I) is communication allowing vehicles to share information with units supporting the highway system. Such units include cameras, tolls, traffic lights, street lights, and parking meters. V2I can be used to automate current payment processes for parking and highway tolls, but also to signal presence to traffic lights and street lights.
- Vehicle-to-network (V2N) communication can be used to broadcast messages from the network to vehicles in the area. These kinds of messages can be warning indications of obstacles or traffic congestion far ahead.
- Vehicle-to-pedestrian (V2P) communication warns cars about approaching pedestrians or cyclists. V2P communication tries to add safety by predicting the upcoming collisions based on position, speed, and direction information exchanged.
- Vehicle-to-vehicle (V2V) communications is a wireless transmission between cars close to each other. The main goal is to prevent accidents by allowing cars in transit to share location and brake sensor data with each other. The cars will create an ad hoc mesh network that allows messages to hop from a car to the next one. For example, an emergency braking of a leading car will broadcast a message that the following cars will react to by applying a brake in a matter of milliseconds.

When automated cars are attempting to identify surroundings and map the environment, they can use the received broadcast messages from other entities instead

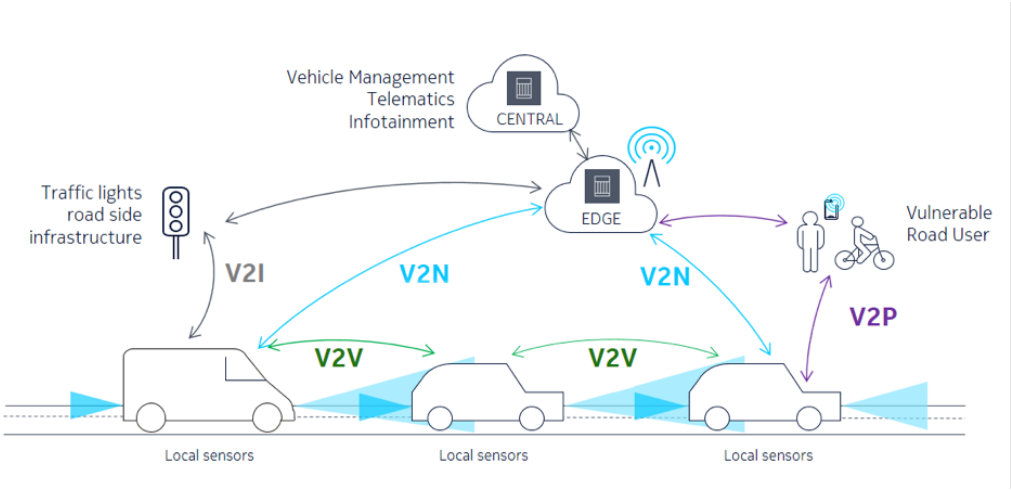

Figure 8: Smart city infrastructure [27]

of the built-in sensors and cameras of the car. Connected cars can detect upcoming, even yet invisible, dangerous traffic situations such as approaching rescue cars or stationary cars parked on the street and initiate appropriate countermeasures. V2X pilots are applied in multiple cities around the world with major car manufacturers engaged. Due to the real-time applications of V2X, it requires minimum latency, high reliability, and high availability from the connection. [22, 33]

The proposed underlying technologies for V2X are Wi-Fi-based and cellular-based (C-V2X) ones. Wi-Fi-based V2X was introduced in 2012, and it supports short-range communication between entities close to each other such as vehicles (V2V) and infrastructure (V2I). Wi-Fi, however, has some limitations on communication range, reliability, security, and throughput. C-V2X has been proposed to displace the Wi-Fi-based solution that was introduced earlier. Based on recent research, the C-V2X outperforms all other standards in terms of reliability, range, latency, and data rates [43]. European Commission has plans to push Wi-Fi as the technology of choice for connected cars over 5G [44]. However, taking into account the Wi-Fi's lack of performance against C-V2X and security vulnerabilities in the authentication [10], C-V2X should be preferred as the main technology for V2X communications.

4.2 Automated driving

Today's cars are already equipped with advanced driver assistance systems such as adaptive cruise control, reversing assistant [34], traffic sign recognition, and lane departure warning [2, 22]. The driver assistance functions are helping the driver in more straightforward tasks and warn about upcoming hazards, but not yet taking full control of the car. The levels of autonomy are declared by the Society of Automotive Engineers (SAE). There are in total of six levels of automation described in Figure 9.

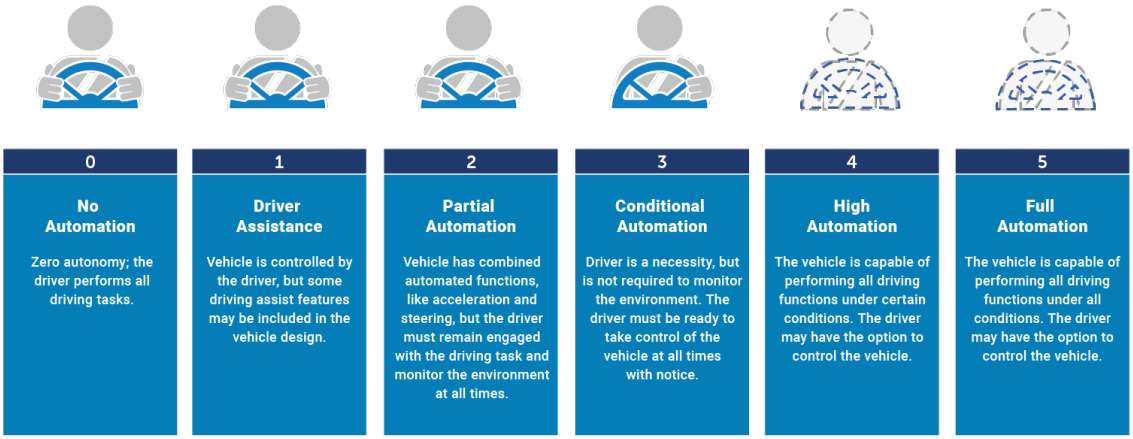

Figure 9: Levels of automation, according to SAE [35]

The list of six different levels of autonomy, according to SAE.

- Level 0 car is fully manual, and the driver is in full control of the car all the time. The driving can be assisted with warnings or interference systems like blind-spot pointers or reversing radars.
- Level 1 automation helps the human driver in a specific driving task such as acceleration or steering with cruise control or lane correction technology. Level 1 cars usually never take over both functions simultaneously.
- Level 2 automation takes over both steering and acceleration/braking functions in easier situations such as cruising on the non-congested highway or driving on quieter roads with great visibility. Level 2 automation guides cars to stay on the lane and can help with acceleration and deceleration or has self-parking features. Regardless of the automation functions, the driver is expected to have control of the car all the time. Tesla's Enhanced Autopilot is one example of the described autonomy.
- Level 3 automation can perform dynamic driving tasks, such as traffic jam chauffeur. This is automated driving on the same lane while adapting to the speed of surrounding traffic, with the expectation that a human driver will respond appropriately to a request to intervene.
- Level 4 automation takes full control of the car, and no driver interaction is needed. In the case of a system error, the level 4 car can stop itself. The cars will be able to handle driving to a predefined destination in most use-cases but might have problems with exceptional environments such as powder snow or off-road. The cars are equipped with pedals, wheels, gas, and brake pedals to grant control to human drivers when needed.
- Level 5 automation equipped cars are completely automated, and no human involvement is needed in any other cases besides deciding the destination. No

pedals, wheels, gas, and brake pedals are installed; thus, the design has been made to maximize space for passengers or serve various functions such as meeting rooms [24, 36]. [37, 38]

This Bachelor's thesis focuses on cars that are automated by levels 4 and 5. The current development of the majority of automated cars is restricted up to level 3. Some level 4 and 5 cars are tested in controlled and restricted environments where the mapping of roads and conditions are up to date with changing elements limited to a minimum. These are environments such as closed roads and parking halls.

4.3 Mobile network requirements

Current automated cars with LTE-connectivity have been able to transmit selected data, such as location, speed, and turning angle to the network to be used for automated driving. However, automated cars are producing an enormous amount of data through the multiple sensors and cameras that the LTE-network throughput is not able to cope with. On top of the sensor data, automated cars are using data for various applications such as infotainment and safety functions. Due to the nature of applications' data usage, the requirements for each connection are different. Infotainment such as streaming multiple video inputs simultaneously, requires high data throughput without the need for low latency or high reliability. Safety functions require high availability, ultra-low latency, and high throughput if uncompressed data streams are used. Automated driving will increasingly demand more and more reliable network-based structures, requiring redundant, real-time architectures [22]. [39]

An increasing number of sensors, inside and outside the car, are producing an enormous amount of data every second. Based on some estimates, each automated car uses up to 4 terabytes per day [40], requiring data rates far beyond 12 Gbps [22]. Currently, cars are processing the data mostly with onboard computers. To improve the driving experience cars withdraw the data to servers and platforms offering maps or crowd-sourced data such as Waze.

A crucial prerequisite for safe automated driving is the real-time transmission of data with ultra-high availability and reliability. Current standards such as LTE based mobile communications can deliver communication with a latency of 30-40 milliseconds, which is not sufficient enough to fill the requirements for real-time transmission. Developers of automated driving functions are focusing on implementing the technology on the 5G standard. The 5G is capable of offering communication with very low latency, less than 1 ms, and with high availability up to 99.9999% with URLLC slice as mentioned in subsubsection 3.0.4 thus filling the requirements of automated driving.

Network slicing included in 5G enables applications with different network requirements to be served by a single base station. With the use of the eMBB and URLLC slices, automated cars can stream infotainment, communicate with roadside infrastructure, and maintain automated driving specific functions such as radar and video stream analyzing with the help of MEC.

5 Security

Automated and connected cars have high requirements for the network, such as high throughput, high availability, and ultra-low latency. To achieve these diverse performance metrics, the 5G technology incorporates several new technologies that will improve the performance specifications and usability of mobile cellular networks. The adoption of new technologies such as MEC, virtualization, network slicing, and CUPS creates new attack surfaces that service providers need to address in the security architecture. Some projects, such as H2020 Caramel [41] has been launched to fill the cybersecurity gaps not addressed yet. Implementing robust and secure end-to-end data transmission is a crucial factor in critical communications and automated transportation. For example, the 5G platform will enable large-scale IoT applications such as the traffic sensors and car-to-infrastructure (V2I) services that are the foundation for smart cities. It is critical that malicious actors cannot access that data, disrupt services, or hijack IoT devices. Though the diversity of the 5G applications and their ever-increasing performance requirements make it challenging to balance the efficiency of security management and security policies. [12]

The cellular network architecture consists of three main entities, as demonstrated in Figure 10. First, User Equipment (UE), typically a smartphone or an IoT device equipped with a Universal Subscriber Identity Module (USIM), is carried by subscribers, the end-users. Second, Home Networks (HNs) contains a database of their subscribers and are responsible for their authentication. However, subscribers may be in locations where their corresponding HN has no base station, for example, when roaming. Therefore, the architecture has a third entity: the Serving Networks (SNs) to which UEs may connect to. SN provides services once both the UE and the SN have mutually authenticated each other and have established a secure channel with the help of the subscriber's HN. The UE and SN communicate over the air, while the SN and HN communicate over an authenticated, wired, channel. [5]

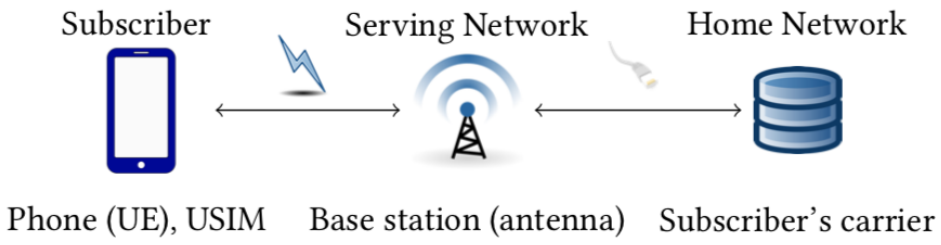

Figure 10: Overall cellular mobile network architecture [5]

This Bachelor's thesis focuses on examining the potential security threats and plausible action points in the 5G transmission channel between UE, the end-user, and the HN. The specifications of the 5G platform are the requirements specified in the Release 15.

5.1 Authentication

Users of the mobile communication networks are authenticated with a successful handshake before any actual data packets are sent back or forth. This authentication is required in roaming to recognize the subscribers' carrier, but also in general required to track and log the data usage for billing purposes. The mobile network protocols enable the subscribers and the HNs to mutually authenticate each other and let the subscribers and the SNs establish a connection with a session-specific key. [5]

The authentication in the 5G standard, based on Release 15, is based on the new versions of Authentication and Key Agreement (AKA) protocols, standardized by the 3GPP. This 5G AKA protocol is an enhanced version of the Evolved Packet System Authentication and Key Agreement (EPS-AKA) protocol, currently used in the 4G technology. The new protocol supposedly provides improved security guarantees compared to the previous version. However, a study on the authentication protocol, using symbolic models to test the logical properties, found out that the security goals are underspecified. The lack of precision in the standard creates logical defects that enable weak agreements between parties or permit replay attacks. In a replay attack, the attacker observes one 5G AKA authentication session and later replays the SN's message to another subscriber. Based on the subscriber's answer, the attacker can distinguish between the subscriber observed previously and a different subscriber. This attack can be used to track subscribers over time, thus violating the privacy properties of the networks' users. The 5G AKA protocol also has a lack of binding properties for an established connection. This flaw allows an attacker to make the HNs bill someone else for the services he is consuming from SN. [5]

The study also found that some authentication properties between the subscriber and SN are implicit, thus not requiring authentication from subscribers' point of view towards the SNs. This lack of authentication could permit a malicious or a fake base station to impersonate a genuine SN towards the subscriber. [5] These malicious base stations could interfere with the connection of automated cars and try to block the connection attempts.

5.2 Network slicing

Varying service slice performance profiles have a direct impact on security protocol choices and policy implementation. Network slices enable a single base station to host multiple diverse network profiles simultaneously. For instance, the first slice could be an eMBB slice serving local subscribers and the second slice hosting critical communications slice used for emergency services. The first slice is open for all subscribers, whereas the second slice is highly privacy-sensitive, requiring intensive security procedures such as frequent reallocation of temporary identities. [12]

A likely model is to run applications requiring MEC on the same physical platforms as other VNFs. These hosted MEC applications may be third-party applications, not controlled by the mobile service provider. This relation raises the concern that poorly designed applications might offer hackers a gateway to infiltrate the distributed

data center and affect the network functions running on the platform. Malicious applications also might try to exhaust the resources needed by the other network functions running in the same network. [12]

One of the main security concerns involves bad actors gaining access to the other slices via a lower security slice. This breach could allow attackers to access the network, including possible MEC resources and traffic of the other subscribers. Attackers also could insert malicious applications to take over the whole platform. This attack vector might gain the bad actor a way for eavesdropping, spoofing, or data traffic manipulation. The network orchestration tools, user authentication, and separation of the slices need to be tested thoroughly before implementing into production in order to block the possible attack vectors. [12]

5.2.1 Distributed Denial-of-Service

One of the key performance initiatives of the 5G protocol is to increase the bandwidth and allow connectivity for hundreds of thousands of IoT devices locally. With the rise of IoT, connected devices are becoming a preferred target for hackers due to the massive scale and generally limited security capabilities. These targeted IoT devices, together with higher network performance capabilities offered by the 5G technology, will create an even more robust network for generating massive attack traffic from the compromised devices. These botnet attacks are known as distributed denial-of-service (DDoS) attacks that are usually targeted towards public services such as banks and government websites, accounting for financial and reputation harm. [12]

In the case of DDoS attacks, suspicious traffic can be redirected to a scrubbing center. However, redirecting adds latency and imposes high financial costs, since backhaul costs are directly tied to the volume of the data traffic. [12]

5.3 Cellular-Vehicle to Everything

Smart city entities such as cars, pedestrians, and infrastructure are connected to each other in V2X. The connection can be established with short-range communication methods such as Wi-Fi or cellular connection. The cellular connection is called Cellular-V2X, where all connections are established via a public cellular network. C-V2X aims to resolve the blockers limiting the usability of traditional V2I networking. C-V2X will especially lower the number of entities involved in vehicular communications and allows the involvement of cellular-security solutions to be applied to V2X [42]. Current applications are deployed using LTE-technology. In contrast to LTE-V2X, 5G-V2X is a function based architecture, which primarily focuses on providing service-based accessibility to the involved entities. The key advantages of 5G-V2X are service-based policing for applications, high performance, and functional support for V2X [13]. 5G-V2X supports edge computing, which is an integral aspect of V2X services.

Automated cars sense the environment and navigate by using real-time data and instructions from different sensors that are connected to the cellular network.

The guidance maps for real-time coordination can be accessed through C-V2X communications. The security features C-V2X helps to prevent impersonation and replay attacks, which may try to misguide the car leading to accidents. The security considerations and applying several key-based mechanisms can help to provide strong encryption for transmissions, including critical data to automated cars [42].

V2X can be operated in Standalone-5G (S-5G) and Non-Standalone 5G (NS-5G) mode. This mode depends on the deployment of the initial architecture. NS-5G-V2X is dependent on the underlying LTE-development to facilitate the requirements required by the 5G standard. Using NS-5G mode limits the scope for enhancements that can be made to the deployment. In contrast, Standalone-5G provides a broader scope to enhance security policies. When using NS-5G for V2X, the attacks possible on LTE-V2X also hold true and are possible to exploit the services in 5G-V2X. With S-5G, the attack scope decreases, and the protection against threats can be enhanced while maintaining performance [42].

Network planning and deployment play a key role in deciding the security of 5G-V2X. The security in 5G-V2X not only depends on the security functions but also on the location of certain functions. Control over any of the network core functions such as User Plane Function (UPF), Access and Mobility Management Function (AMF), and Session Management Function (SMF) exploits the whole network. Thus, it comes fundamentally necessary to secure the routes between entities. It is worth noting that the placement of functions and control is a balance between performance and security. The positioning of the servers providing security functions must be carefully selected. A security anchor function near to the user may lead to several client-side attacks while placing at the core increases the latency and weakens links between the core functions [42].

The primary security of 5G-V2X is defined using 5G-AKA through a hierarchical key distribution. The authentication was discussed previously in subsection 5.1. V2X authentication and securing the credentials are the key issues to be considered for 5G-V2X. Moreover, network layout and planning are yet to be fixed.

6 Conclusions

The 5G mobile communication technology that is about to be harnessed into use during 2020 has been an anticipated evolution of the currently used 4G technology. The extensive performance and multiple new services are enabling innovations in multiple different verticals. Autonomous and connected cars are one of the verticals that benefits from this technological leap.

The first question in this Bachelor's theses was to evaluate if the 5G technology offers sufficient performance for the fully automated, SAE level 4 and 5, and connected cars. Modern automated cars are requiring reliable and low-latency data transfer from the communication channel to exchange information with other entities. With the help of network slicing, the 5G network can be split into different data profiles serving customers with various needs simultaneously. The URLLC slice will serve the end-users with ultra-low latency and highly reliable communication that is required by autonomous cars to communicate with smart city infrastructure. The eMBB slice offers high data throughput that can be used to transfer data-intensive sensor input to the cloud for further analysis. The services, such as MEC can be used to process or store the data close to the end-user with low latency. This service can be highly beneficial to examine sensor data gathered by an autonomous car. The 5G protocol also offers new services to support connected cars such as vehicle platooning and remote driving.

The improvements in the performance and changes in the services and require changes in the network architecture compared to the 4G technology. These changes, however, are adding challenges to the network design, especially to the security of the network. The pressure to deliver high performance might lead to compromises for the security and privacy of the network. For example, extensive authentication adds latency and limits the throughput of the communication. The architectural changes might also open up unexpected attack surfaces in services such as network slicing.

In the last part of this Bachelor's thesis focus was on the security features of the proposed 5G protocol. The proposed authentication protocol 5G-AKA was found to be prone to replay attacks. These attacks might lead to exposure of the end-users location, thus violating the privacy feature. The lack of authentication also could permit a fake base station to impersonate a genuine base station towards the end-user leading to compromise of end-to-end encryption. Extensive data throughput with the combination of high device density in the network gives the possibility for more extensive DDoS attacks. The lack of data scrubbing and filtering for unwanted traffic needs to be addressed before implementing public 5G to its full capacity.

The 5G protocol is still a work in progress and is about to be finished during the year 2020. Authentication and security is the biggest challenge that needs to be addressed before implementing the network into full use. End-users and critical services such as smart city applications need to be provided with the required privacy and security level. The network layout needs to be tested thoroughly before taking into full use with the focus on security and privacy that needs to be the top priority when introducing new technologies.

References

[1] An, X., Zhou, C., Trivisonno, R., Guerzoni, R., Kaloxylos, A., Soldani, D., Hecker, A. (2017). *On end to end network slicing for 5G communication systems.* Transactions on Emerging Telecommunications Technologies, vol. 28, no. 4, pp. e3058.

[2] The Tesla Team. (2016). *All Tesla Cars Being Produced Now Have Full Self-Driving Hardware* [online]. Available: https://www.tesla.com/blog/all-tesla-cars-being-produced-now-have-full-self-driving-hardware [accessed 2019, Mar 17].

[3] Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., Gurtov, A. (2017). *5G Security: Analysis of Threats and Solutions.* IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki.

[4] Deloitte. (2017). *5G mobile – enabling businesses and economic growth* [online]. Deloitte Access Economics. Available: https://www2.deloitte.com/au/en/pages/economics/articles/5g-mobile.html [accessed 2019, Mar 19].

[5] Basin, D., Dreier, J., Hirschi, L., Radomirović, S., Sasse, R., Stettler, V. (2018). *A Formal Analysis of 5G Authentication.* DOI: 10.1145/3243734.3243846.

[6] 5G World Pro. (2019). *3GPP 5G roadmap and 5G main features (5G training)* [online]. 5G World Pro. Available: https://www.5gworldpro.com/5g-knowledge/82-3gpp-5g-roadmap-and-5g-main-features.html [accessed 2019, August 25].

[7] Li, X. et al. (2017). *Network Slicing for 5G: Challenges and Opportunities.* IEEE Internet Computing, vol. 21, no. 5, pp. 20-27, DOI: 10.1109.

[8] Woyke, E. (2018). *Companies fed up with crappy Wi-Fi are deploying 5G instead* [online]. MIT Technology Review. Available: https://www.technologyreview.com/s/612477/companies-fed-up-with-crappy-wi-fi-are-deploying-5g-instead [accessed 2019, Mar 20].

[9] Nelson, P. (2018). *Private 5G networks are coming* [online]. Network World. Available: https://www.networkworld.com/article/3319176/private-5g-networks-are-coming.html [accessed 2019, May 28].

[10] Kohlios, C., Hayajneh, T. (2018). *A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3* [online]. DOI: 10.3390/electronics7110284.

[11] Marek, S. (2018). *Why CUPS Is a Critical Tool in the 5G Toolbox* [online]. SDxCentral. Available: https://www.sdxcentral.com/articles/news/why-cups-is-a-critical-tool-in-the-5g-toolbox/2018/10/ [accessed 2019, August 26].

[12] Hodges, J. (2019). *5G Security Strategy Considerations* [online]. Heavy Reading. Available: https://www.juniper.net/assets/us/en/local/pdf/whitepapers/2000743-en.pdf [accessed 2019, June 10].

[13] 3GPP. (2018). *Release 15* [online]. The Third Generation Partnership Project (3GPP). Available: http://www.3gpp.org/release-15 [accessed 2019, Mar 19].

[14] 3GPP. (2018). *Service requirements for next generation new services and markets* [online]. The Third Generation Partnership Project (3GPP). Available: https://www.etsi.org/deliver/etsi_ts/122200_122299/122261/15.05.00_60/ts_122261v150500p.pdf [accessed 2019, Apr 11].

[15] Kavanagh, S., Thomas, K. (2019). *What is a private 5G network?* [online]. 5G.co.uk. Available: https://5g.co.uk/guides/what-is-a-private-5g-network/ [accessed 2019, August 22].

[16] The 5G-MOBIX Project. (2019). *Deliverable D2.1 5G-enabled CCAM use cases specifications* [online]. Available: https://www.5g-mobix.com/assets/files/5G-MOBIX-D2.1-Use-case-specifications-v1.0.pdf [accessed 2019, August 30].

[17] Thingsee. (2019). *Thingsee Environment Technical Presentation* [online]. Available: https://thingsee.com/wp-content/uploads/2019/02/thingseeenvironment_technical_presentation_v.19.02.pdf [accessed 2019, Apr 4].

[18] Brown, G. (2018). *Ultra-Reliable Low-Latency 5G for Industrial Automation* [online]. Heavy Reading. Available: https://www.qualcomm.com/media/documents/files/read-the-white-paper-by-heavy-reading.pdf [accessed 2019, Mar 20].

[19] Mehraghdam, S., Keller, M., Karl, H. (2014). *Specifying and Placing Chains of Virtual Network Functions*. DOI: 10.1109/CloudNet.2014.6968961.

[20] Ordonez-Lucena, J., Ameigeiras, P., Lopez, D., Ramos-Munoz, J., Lorca, J., Folgueira, J. (2017). *Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges*. IEEE. DOI: 10.1109/MCOM.2017.1600935.

[21] Sprecher, N. (2016). *Mobile Edge Computing - An enabler for enhanced Car2X communication* [online]. European Standards Organization with Global Impact. Available: https://www.etsi.org/component/rsfiles/preview?path=MEC+Presentations+at+Industry+Events%5C201606+-+Connected+Cars+-+ETSI+Mobile+Edge+Computing.pdf [accessed 2019, August 26].

[22] TE Connectivity. (2018). *The Road to Autonomous Driving* [online]. TE Connectivity (TE) Ltd. Available: https://www.te.com/global-en/campaigns/transportation-solutions/connected-car-2-form.html [accessed 2019, Jan 27].

[23] Bloomberg. (2017). *Wuhu, CN is piloting AVs* [online]. Bloomberg Group. Available: https://avsincities.bloomberg.org/global-atlas/asia/cn/wuhu-cn [accessed 2019, Apr 13].

[24] Geek.com. (2019). *World's First All-Weather Autonomous Bus Rolls Out in Finland* [online]. Geek.com. Available: https://www.geek.com/tech/worlds-first-all-weather-autonomous-bus-rolls-out-in-finland-1778855 [accessed 2019, Apr 14].

[25] Sensible 4. (2019). *GACHA – Self-driving shuttle bus for all weather* [online]. Sensible 4. Available: https://www.sensible4.fi/gacha [accessed 2019, May 28].

[26] Saxen, T. (2018). *Self-driving cars will be supported by 5G networks* [online]. Telia. Available: https://www.telia.fi/business/article/5g-comes-in-support-of-self-driving-cars [accessed 2019, August 30].

[27] Marin. (2019). *Nokia, Telia and Sensible 4 are testing an autonomous 5G equipped vehicle called Juto* [online]. Nokia. Available: https://nokiamob.net/2019/02/06/nokia-telia-and-sensible-4-are-testing-an-autonomous-5g-equipped-vehicle-calle [accessed 2019, August 30].

[28] The 5G-MOBIX Project. (n.d.). *The 5G-MOBIX Project* [online]. https://www.5g-mobix.com/about [accessed 2019, August 30].

[29] 5G CARMEN. (n.d.). *5G CARMEN* [online]. Available: www.5gcarmen.eu [accessed 2019, August 31].

[30] 5GCroCo. (n.d.). *5GCroCo* [online]. Available: www.5gcroco.eu [accessed 2019, August 31].

[31] AB Volvo. (2016). *Volvo first in the world with self-driving truck in underground mine* [online]. Volvo Group Press. Available: https://www.volvogroup.com/en-en/news/2016/sep/news-2297091.html [accessed 2019, Apr 13].

[32] RAC. (2019). *RAC Intellicar* [online]. RAC. Available: https://rac.com.au/about-rac/advocating-change/initiatives/automated-vehicle-program/intellicar [accessed 2019, Apr 13].

[33] Whyte, W. (2016). *IEEE 1609.2 and Connected Vehicle Security: Standards Making in a Pocket Universe*. DOI: 10.13140/RG.2.2.30133.88802.

[34] Patrascu, D. (2018). *How the BMW Reversing Assistant Works* [online]. Autoevolution. Available: https://www.autoevolution.com/news/how-the-bmw-reversing-assistant-works-129885.html [accessed 2019, May 28].

[35] NHTSA. (n.d.). *The Road to Full Automation* [online]. National Highway Traffic Safety Administration. Available: https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety [accessed 2019, August 23].

[36] RAC. (2019). *RAC Intellibus* [online]. RAC. Available: https://rac.com.au/about-rac/advocating-change/initiatives/automated-vehicle-program/intellibus [accessed 2019, Apr 14].

[37] Chatterjee, V. (2018). *Society of Automotive Engineers (SAE) Automation Levels for cars* [online]. Automotive Electronics. Available: http://www.automotivelectronics.com/sae-levels-cars/ [accessed 2019, Apr 14].

[38] SAE International. (2014). *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems* [online]. SAE International. Available: https://www.sae.org/standards/content/j3016_201401/ [accessed 2019, Apr 14].

[39] TE Connectivity. (n.d.). *6 Key Connectivity Requirements of Autonomous Driving* [online]. Available: https://spectrum.ieee.org/transportation/advanced-cars/6-key-connectivity-requirements-of-autonomous-driving [accessed 2019, Jun 6].

[40] Nelson, P. (2016). *Just one autonomous car will use 4,000 GB of data/day* [online]. Network World. Available: https://www.networkworld.com/article/3147892/one-autonomous-car-will-use-4000-gb-of-dataday.html [accessed 2019, Apr 14].

[41] H2020 Caramel. (n.d.). *H2020 Caramel* [online]. Available: https://www.h2020caramel.eu [accessed 2019, August 30].

[42] Sharma, V., Lee, Y., You, I. (2019). *Security of 5G-V2X: Technologies, Standardization and Research Directions*. arXiv:1905.09555v1 [cs.NI].

[43] Anwar, W., Franchi, N., Fettweis, G. (2019). *Physical Layer Evaluation of V2X Communications Technologies: 5G NR-V2X, LTE-V2X, IEEE 802.11bd, and IEEE 802.11p* [online]. Hawaii, EEE 90th Vehicular Technology Conference (VTC-Fall 2019).

[44] Morgan, S. (2019). *Bulc urges 5G advocates to focus on autonomous driving, leave connected cars to WiFi* [online]. Euractiv. Available: https://www.euractiv.com/section/road-safety/interview/bulc-urges-5g-advocates-to-focus-on-autonomous-driving-leave-connected-cars-to [accessed 2019, Aug 30].