# *Statistical in-depth security analysis for Vehicle to everything communication over 5g network*

**Rejwan Bin Sulaiman**

School of *Computer Science* and Technology
University of Bedfordshire
Vicarage St, Luton LU1 3JU

**Ranjana Lakshmi Patel**

School of *Computer Science* and Technology
Northumbria University
2 Sandyford Rd, Newcastle-upon-Tyne, NE1 8SB

# Abstract

Many researchers have invested their time, effort, and energy on the research area of "Vehicular-to-everything" which is also known as V2X in term of security and vulnerabilities. For communications like V2X, the European Telecommunications Standards Institute (ETSI) has been engaged in order to formulate quality standards for these types of the methodological communication system. The Wi-Fi protocol 802.11p has no capability to offer any sort of security and privacy of data. However, upon the development that took place in the field of 5G technology, now many companies, as well as researchers, have locked the attention to use this technology so that the V2X communication can serve the people with better security and protect them from the harmful acts. If the 802.11p can be exchanged with the 5G, it will surely bring advancements to the ETSI security mechanisms. Nevertheless, it is possible to have counterattack from the new features that will have been installed. It will be made sure that the attacks can be encountered with efficiency rest assured. This thesis stands for taking a point on the aspects of Statistical in-depth security analysis for Vehicle to everything communication over 5g network and how 5G can put effect on the security of the communication. In this thesis, it has been investigated that it is not impossible to make a transit from the 802.11p to 5G NR in term of security aspects. However, it needs some alteration in the protocol stack. That is why different types of improvements have been proposed in this thesis so that the security mechanisms will get stronger and better. The advancements due to the improvement will eradicate the present certificate mechanism which is needed for the authentication. This will be done only because the prospects and aspects of 5G will provide the communication with so many features that authentication will not be needed in that regard. In the end, the positivity and negativity of the introduction of 5G in V2X communication will be discussed along with further recommendations.

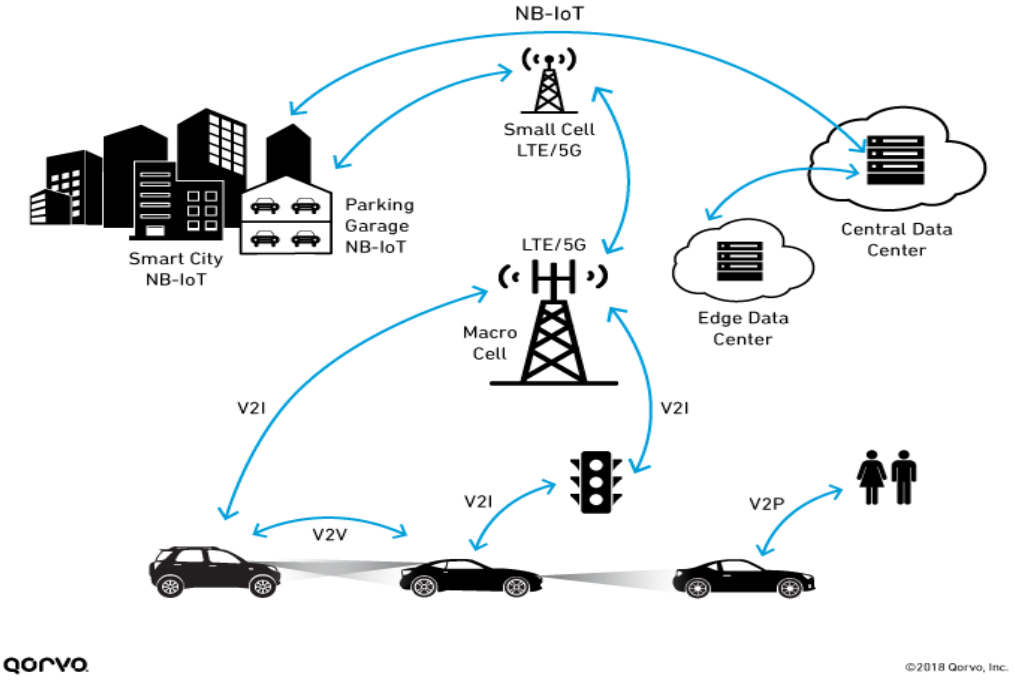
**Keywords:** vehicle to vehicle communication, V2X communications, V2X communication over 5G, 802.11p, network security, ETSI, ITS, security architecture, connected car; vehicular network security mechanisms, remote diagnostics

# Table of Contents

# 1

# 1 Introduction

The researchers, as well as many companies, have put a lot of attraction on the vehicular network and the impact of 5G in V2X communication. The European Telecommunications Standards Institute (ETSI) is responsible for coming up with a standard Vehicle-to-Everything (V2X) in order to shape up an Intelligent Transport System (ITS). The standards have inclusion of a protocol stack, security mechanisms, security requirements, and architectural stability. ( European Telecommunications Standards Institute, 2010 )




For V2X communications, Long Term Evolution (LTE) has been investigated by the 3rd Generation Partnership Project (3GPP so that it could be used in order to check the possibility to do so.( European Telecommunications Standards Institute, 2004,2009 ) Unlike LTE, the “LTE advanced” was capable of fulfilling the IMT-Advanced requirements for the 4G. Again, in order to come up with the standards, the ETSI has been responsible for the augmentation of LTE for the V2X communications.( European Telecommunications Standards Institute, 2017 ) On the other hand, the ETSI ITS standards have been fitted compared to the LTE V2X communication (Filippi, et al 2017). Efficiency, speed and reliability- the mash-

up of these three is about to happen due to the advancements of 5G New Radio (NR) technology which is far better than all the technologies related to the segment. In 2015, the advancements of 5G started to take place and afterwards, the overall standards have been re-organized so that it can provide the necessary support to the traditional cellular networks with different types of endnotes such as cooperative vehicles and IoT (5G Automotive Association,2016). High speed, as well as broad bandwidth, can be gained with the assistance of 5G NR technology.

That being said, one important notion has not been taken into account and has not been vested with time and energy by the researcher to dig up. They have not paid much attention to know how 5G put an impact on the security of V2X communications. It is expected that the new introduction of technology surely comes up with different types of security hurdles. Nevertheless, 5G has the potential to bring about new possibilities to protect and secure the vehicles and to provide security mechanisms in ITS model.

This thesis can be regarded as the complements of the research on the Statistical in-depth security analysis for Vehicle to everything communication over 5g system of the EU 5G Infrastructure. In addition, it can be related to the different types of V2X projects at the Chalmers as well as the FFI/Vinnova projects. VolvoAB and the Corporation of Volvo Car concentrate on augmenting the privacy and the security for the future vehicles which will be run and operated by the future generation. Hence, the main point of this whole thesis will be to amalgamate the viewpoint of the researchers on in-depth security analysis on 5G for Vehicle to everything communication as well as the viewpoint on the security of ITS stack.

## 1.1 Aim of the thesis

The thesis has an aim to address which is to investigate the Statistical in-depth security analysis for Vehicle to everything communication over 5g network and security effect of V2X communications upon assisted by 5G technology that has already been defined by the ETSI. To do so, security improvements, as well as vulnerabilities, have been checked as well as examined to have a further view on the research topic. In addition, important reductions have been explained which is needed to define the protocol stack accordingly.

## 1.2 Motivation and research questions

At present, 802.11p is being used in all link-layer protocols with respect to the V2X communication system. However, this possesses a lot of hurdles such as it has no security, to begin with. Since the advancement of 5G is taking place accordingly with the time, thousands of companies and researchers have put their eyes on the usage of V2X communication upon assistance with the 5G technology. There are features which do

not resemble the 802.11p in 5G NR and these features provide new possibilities to the feature. In the meantime, vulnerabilities kick in from the other side. To be more specific, the executed security mechanisms belong to the higher up which holds the possibility to become exchanged by the functionality of 5G. Hence, the executed mechanism might become useless or redundant at times. Nevertheless, there are many features which will provide upgraded security and protection to the people and this has been placed in this thesis.

Five research questions have been formulated in order to explain the thesis in an organized manner:

- RQ1: What type of security mechanisms and protocols has been considered in ETSI V2X communications till now?
- RQ2: What type of security requirements are needed for several use cases of ETSI ITS?
- RQ3: What are the features that can be utilized at the physical layer in order to develop the security measures of 5G? Is it possible to repudiate any security mechanism from the higher layer protocols?
- RQ4: What are the vulnerabilities that 5G NR can cause to V2X communication?
- RQ5: Will it be possible to replace 802.11p with 5G NR? What are the stymies if it is not possible to replace?

## 1.3 Scope

This thesis has limitations since it has been restricted by different types of resources such as time and availability of data. Scopes of doing the thesis are given below:

- This thesis can be and should be considered as a general study which will not possess a detailed analysis of the execution of several types of protocols. In this thesis, the protocol stack and the associated relevant topic has been discussed to provide an overall view on the research topic.
- The abstractions have been originated from the execution of 5G NR and 802.11p protocols. In terms of security perspective, this thesis only provides the germane information to investigate the differences between them.
- Since the time has been an issue, it was not possible to have the inclusion of a new protocol stack like the integration of 5G into ITS stack.
- The target of this thesis is to find out whether the replacing of 802.11p can be done with the 5G. Neither the associated problems have been taken into account, nor the solution of the problems.

In the end, this thesis does not have any intent to provide the best optimization system for all security mechanisms. However, the goal is to collect the information so that the localization of all the possible optimization can be done.

## 1.4 Research Flow

For the purpose of writing this thesis, we have first Identified the research questions. And later to resolve or to get answers to the questions we have performed a deep research on the existing technologies. These include the security analysis on the current ETSI ITS protocols, security standard and the 5G network model that is existing now. Most of the papers that we have read could be found in the IEEE explorer. As there are lot of work done in this field, we have also contracted the field experts and the academics for interview purpose. These helped us to gain in-depth knowledge and based on that we have analysed different elements of 5G networks in the V2X communication.

Finally, we have critically analysed our research questions with the existing technology and also compared to the different possible obstacle that might become to adopt with the recommended technology.

## 1.5 Overview

This report is structured as mentioned. At the beginning of the thesis we have gathers all the research study that is existing and relating to our research, we described that as a Literature review in chapter 2. We have divided this chapter into the different parts as the culture of the research. In the third chapter we described our methodology in-depth and how we adopted to acquire this thesis. The fourth chapter is all about the analysis of the gained knowledge, comparative study and critically analysis of the different security topics. We also discussed what could be adopted and what we can avoid. We conclude the thesis by the fifth chapter with recommendations for future works and conclusion.

# 2

# 2 Literature Review

## Introduction

The technological transformation is taking place in the automated vertical market with a view to creating more concentrated vehicles with full automated capacity. It is possible to do so with the assistance of 5G. This can be done on the basis of the connection between the autonomous vehicles incorporate with each other by taking into consideration of the Vulnerable Road Users (VRUs), vehicle-to-everything (V2X) in 5G network system. V2X is capable of formulating the perception of the environment. Thus, it possesses the potential to come up with right decisions by exchanging views among the vehicles close to the environment. The automated vehicles can ensure safe transportation system which can drop down the fatality rate minimal. In addition, traffic congestion will be smoother and the impact on the environment will encounter less impact. However, the challenges persist and to have found the answer of the research questions, 5G, 5G NR, ETSI ITS and the IEEE WAVE standards, and cellular V2X have been discussed.

## 2.1 The Vehicular network standards

### 2.1.1 ETSI ITS

Different types of standards have been devices with respect to the ITS communication (ITSC). The standards have inclusion regarding the protocol stack(Gianotti, et al., 2016); the communication architecture (Visala, 2014); security requirements as well as the messages (Visala, 2014)and the architecture and services. The end nodes in those standards are known as the ITS station. The vulnerability and the execution assessment are needed to be done in the upcoming sections.

### 2.1.2 IEEE WAVE standard

The Wireless Access in Vehicular Environments (WAVE) has been introduced by the IEEE on the basis for V2X communication (Ahmed, Ariffin, & Fisal, 2013). It was, in the beginning, in the United States. The WAVE has been undertaken with a view to demonstrating several standards which are needed for V2X communication. With respect to the security and architecture, WAVE is quite close to the European standard. In the WAVE stack, the colours are responsible for the demonstration of the ETSI ITS layers. In the upper layers, the difference can easily be discovered since the WAVE Short Message Protocol (WSMP) is utilized in lieu of the GeoNetworking or the BTP in ETSI ITS standards.according to (Ahmed, Ariffin, &Fisal, 2013) this protocol is used for the minimization of the communication overhead. WSMP and UDP services are not clearly defined in the WAVE services. Different types of cryptographic mechanisms such as the public/symmetric keys for signing/encryption, verification of the certificates given by the infrastructure of the authority. The certificates can be of two types such as explicit, which means that the public key is explicit; and implicit, which has an inclusion of a reconstructed value for public key).

# 2.2 5G for V2X

Many types of research have been done on focusing the optimization for V2X communication. According to(Aurora, et al., 2010) authors have come up with a new proposal on the non-orthogonal time-frequency schemes for the allocation so that the achievement can be attained which can ensure high reliability and low latency. In that paper, a creation of the testbed took place for low latency and high-reliability 5G-V2X communication system (A Ali et al, 2017). Another proposal has been proposed by Pak which states that a faster and smoother pack of classification can enhance the performance (wooguil, et al , 2017). However, Chang et al. (2016) proposed another proposal in order to eschew from the flood and storms of the messages by the broadcasts. According to Zhou and Kellerer (2017), this concept of the Virtual Cells (VCs) has the potential to optimize with respect to the efficiency of power, reliability, and capacity. However, Luoto et al. (2017) have found that the optimum performance can be discovered in between the LTE communication of the vehicles which possess with comparatively sophisticated connection server with the RSU. Zou et al. (2017) has come up with another proposal for the emergency braking system and recommended 5G for the usage of the vehicle to vehicle (V2V) . In this paper, it was discussed that the cellular activity is used in analyzing the scenario but it is not used for the Uuinterface. As it has been sufficed in the paper that been written by Boban et al (2016). , the

Global Navigation Satellite System-based (GNSS-based) synchronization has been one of the most important network coverage scenarios to date. The multi-antenna can give good coverage as well as necessary developments related to Ultra Reliability and Low Latency Communication (URLLC). According to the definition given by the ETSI ITS, in the phase of testing, BISSender, BISReceiver, and different layer utility messages were used by the software programs (European Telecommunications Standards Institute,2011). Then the whole pack is delivered to the Radio BBU as a mean of UDP messages which are then sent by the 5G communication through device to device. By doing so, the rates of the messages went up to 200Hz which is normally kept between 1-10Hz.

## 2.3 C-V2X vs 802.11p

The research questions contained the plausibility whether it is possible to convert from 802.11p to 5G NR. It is important to find the differences between them so that the comparison can be made easily. Since 5G NR is still in the process of development, the comparison will be between the 802.11p and C-V2X. The following table depicts the comparison between these two such as:

| 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

Filippi et al (2017) has concluded in a nut shell, the C-V2X has been devised for the V2I/I2V communication which possesses a direct communication. However, in case of the 802.11p, this

has been devised solely for the ad-hoc mode with which different vehicles can be able to make connection and communicating directly. Before setting up a connection, it is advised to add a Basic Service Set (BSS). Though it might not possess any security in 802.11p, the reliability stands on the higher level of security mechanisms. In addition, the 802.11p is not more sophisticated as well as well structured like C-V2X according to Filippi et al (2017).

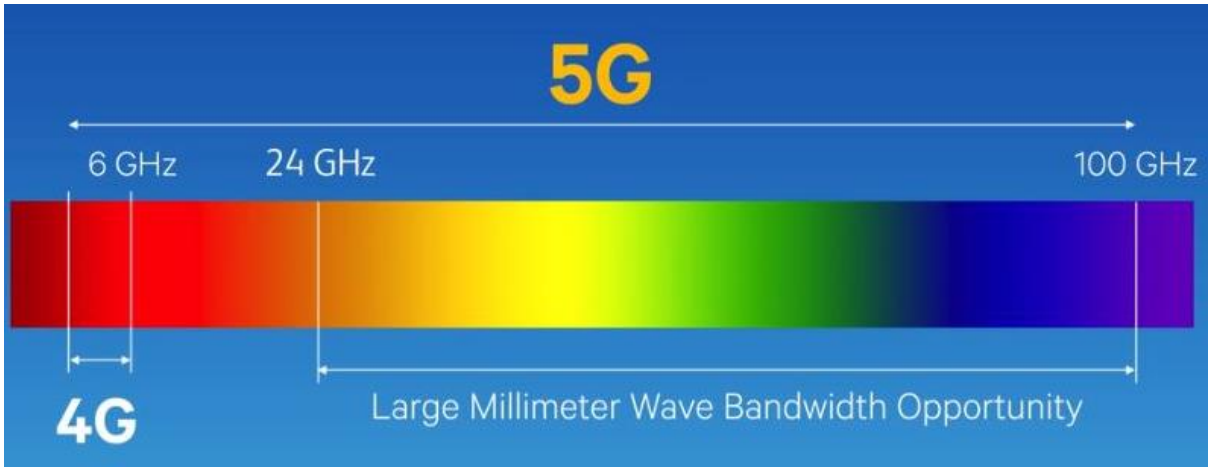
## 2.4 5G NR (New Radio) frequency

5G has the potential to come up with a new technology based on the usage of the radio. This is called NR. NR has been devised so that the communication can take place with different types of systems. In the end of the 2017, NR was released primarily on 3GPP.org (2017) . This has the capacity to provide credible and reliable communication by consuming broader bandwidth. There are also some modern technologies which have been proposed by satrya et al (2017) for the 5G physical layers such as Visible Light Communication (VLC), millimetre wave (mmWave), NOMA, massive MIMO, and cognitive network


## 2.5 mmWave

The LTE radio possesses an optimum frequency up to 2.6GHz. However, the need of more data transmission rates is there to take care of. In order to provide support in this regard, the mmWave can be able to provide a huge spectrum of frequency from 30 to 300 GHz by utilizing a very minimal wavelength of 1-10 mm that is stated by Boban et al (2016). He also suggested that the

size of the antennas has to be decreased and so has the size of the wavelength. The short wavelengths may create hurdles since these do not work in harsh weather Boban et al (2016) added. That being said, to solve the matter, the 5G NR can have inclusion of multi-node beamforming technology.




## 2.6 MIMO and beamforming in 5G

To put reliability on the mmWave technology, beamforming technology can ensure the reliability to great extent. Since the sizes of antennas are small, it is possible to establish several antennas in the base station separately. The multiple-input-multiple-output (MIMO) antenna enables concentrated beams to have an aim at the users who are individual in nature. By utilizing beam tracking as well as beam training, a beam can efficiently provide the users with uninterrupted communication setup through identical links published by Adeshina et al (2017) in a IEEE conference.

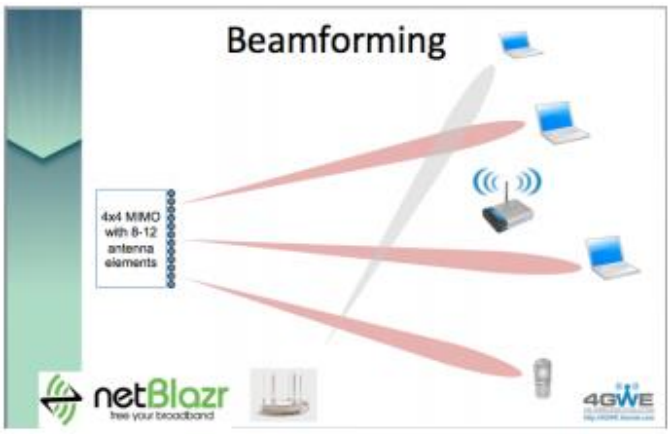
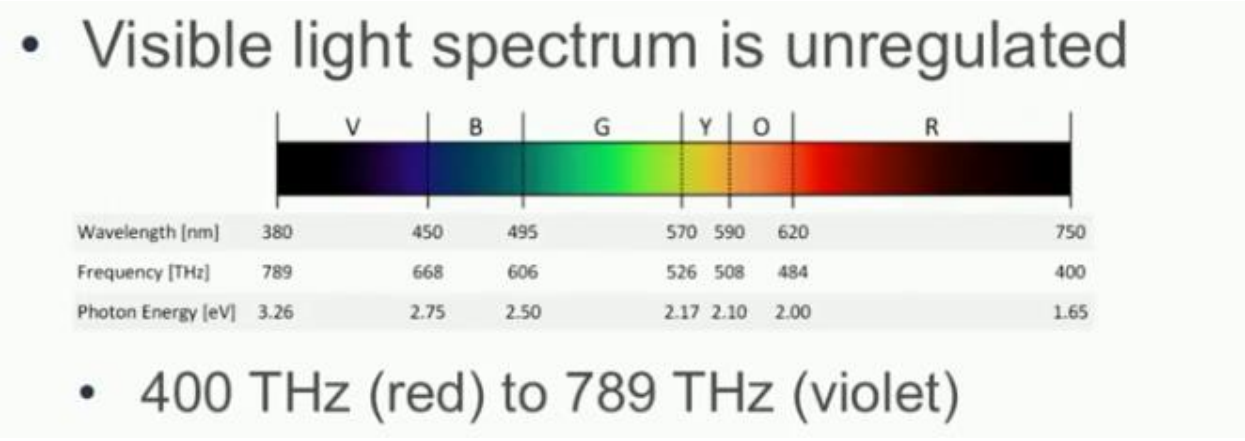



**Figure 2.9:** A visualization of how beams can be formed using massive MIMO antenna arrays

The aforementioned technologies have been investigated with relation to V2X communication. In a paper from Vaet al.(2016), it has been presented that high-quality mobile devices are needed for faster beam training. In prior method, many beam pairs have been used instead of using a single beam. Larsson et al. (2017) have investigated this same phenomenon and here, they executed proficient tracking of beam pairs in volatile situations where the frequency switches remained between all of the points of transmission. An experiment took place on the race track of BMW which has made the researchers more enthusiastic. Emphasis was given on the control of Doppler shifts which has been introduced by high speed. A solution has been proposed by Tateishi et al. (2017) stating that Channel State Information (CSI) can be chosen to minimize the overhead of signalling. Zhao et al.(2017) in another paper came up with an idea for securing the communication system. MIMO signalling, as well as the duplex operation, is supported by the two-way communication system. Al-Momani et al.(2016) on another paper has proposed to have the usage of the beamforming so that the re-authentication of the physical layers can be augmented. A channel called 'signature' is used for the authentication which is amalgamated of different variations in the Doppler shift.

# 2.7 visible light communication ( VLC )

Visible Light Communication (VLC) is attracting many times and efforts of the researchers all around the world. This is regarded as radio transmission which is actually not a significant portion of the 5G NR. This technology has already been used in the RONJA project as a part of early execution of the technology in 2001 according to ronja.twibright.com (2017). This technology has the potential to provide betterment for the execution of 5G developments.

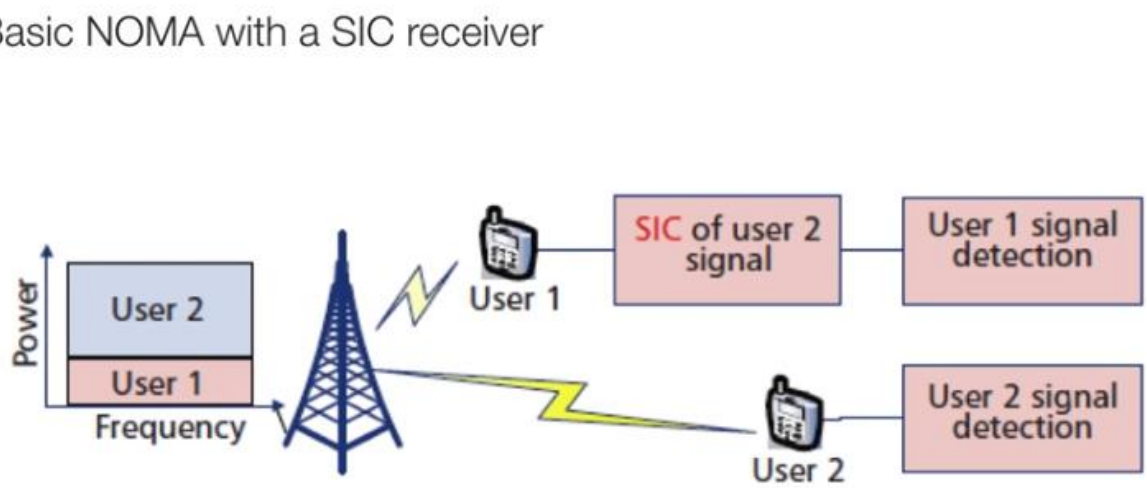



VLC is responsible for transferring data at a very high speed by flickering LED light which naked human eye is unable to comprehend. During the time, if the light is switched on, then it will portray 1 and in case the light is switched off, then it will show 0 respectively Karthik et al (2017)

published.With respect to backhaul communication, VLC system can definitely add value in between national core and cell towers ( Zhao et al , 2017). The benefit of the VLC system lies in the long-distance outdoors. However, there are definitely some challenges in the execution of the VLC system in the long run. One of the benefits of VLC technology is the cost-effectiveness and the greenness it serves to the environment compared to the mmWave. In case for the challenges or the drawbacks, the VLC technology consumes much more expensive due to the rigorous purpose it serves and that is why the operating expense is huge whereas it does not require any expensive devices within itself. In addition, the drawbacks can have inclusion of the low Signal-to-Nose Ratio (SNR) so that the light can spread far away and stay sensitive to the surrounding. Valiveti(2017) came up with a paper which states that the passengers of a train can have hybrid communication system with LiFi/WiFi. This particular system is known as 'grey system' and a central network will be responsible for determining the handover of taking place. This decision is decided by calculating the Signal to Interference Ratio mostly.

## 2.8 Non-Orthogonal Multiple Access (NOMA)

Non-Orthogonal Multiple Access (NOMA) is another method which has the potential to be used in the 5G NR mentioned in Kizilirmak's publication (2016). Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA), and Code Division Multiple Access (CDMA) are the methods are regarded as useful methods that can add value in the scheduling method like NOMA. However, aforementioned methods altogether fall under Orthogonal Multiple Access (OMA) which is unable to provide the cooperation requirement for 5G NR.

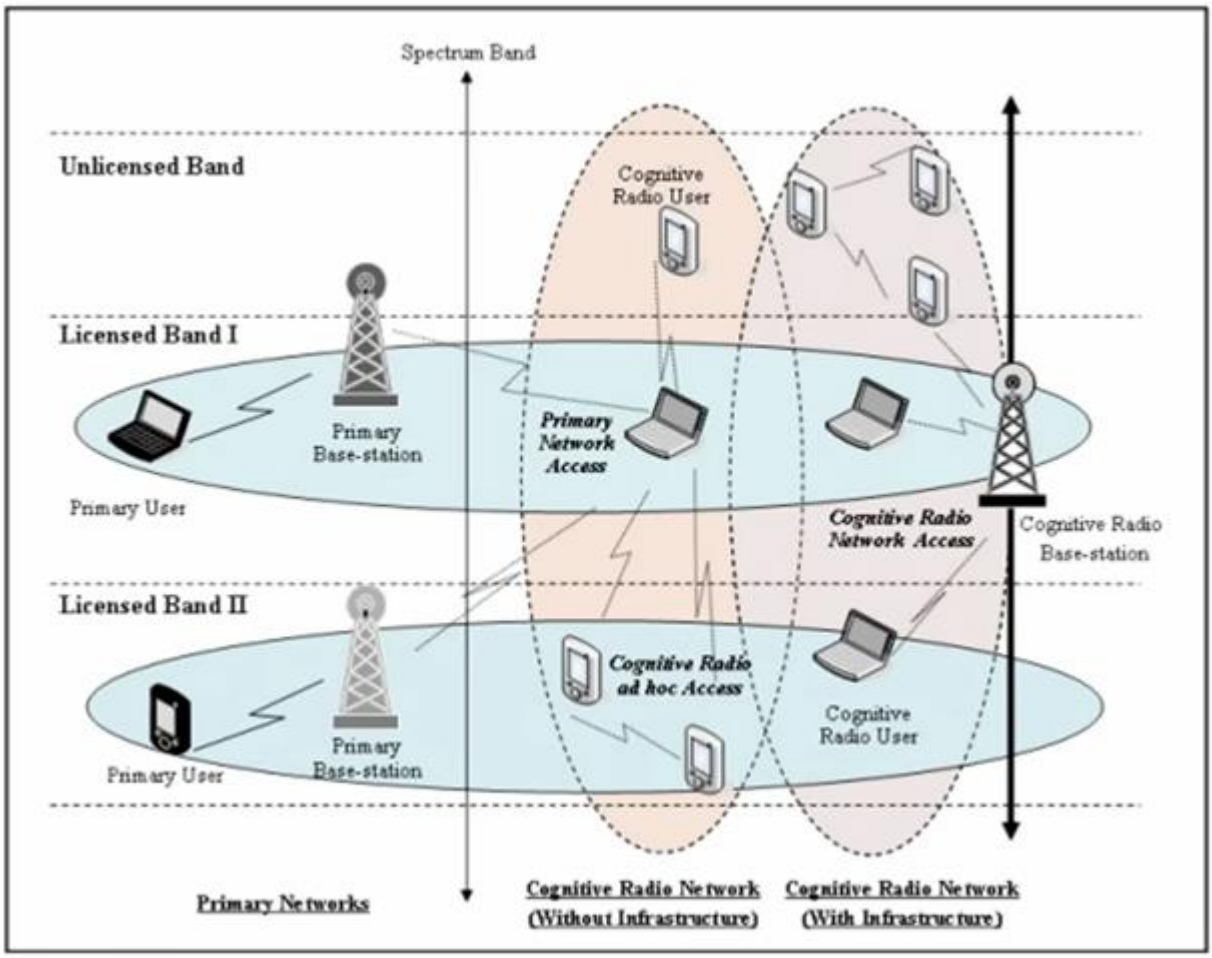



Simultaneously, in case of NOMA, several users can have the capacity to transmit at the same

time using the identical frequency where the signals can be transmitted in the form of a wave by separating the power level of the receivers. The separation is regarded as the Successive Interference Cancellation (SIC). Since the separation needs to be iterative in nature, it is known as the successive where the topmost strong signal is taken for extraction as well as subtraction until the desired signal is revealed. Spectral Efficiency (SE) and Energy Efficiency (EE) can provide high degree of data rate which can only be done provided that the cancellation is perfect after the assumption of SIC. Although in real life, it is close to impossible that the perfect cancellation can take place and it is impossible since there would be some sort of interference that would take place. This is why the data rate is lower due to the remaining of the interference. In fading channels, the errors of the cancellation are expected to be found. One of the problems of using NOMA is the requirement of high computational power which is required for the SIC algorithm in case for running the huge number of enhancement of users. For the vehicles, it will be a hurdle for the optimization of allocating power. With a view to controlling the challenges, it is imperative to accumulate MIMO with NOMA so that the errors will be minimized and the reliability of the combination will increase. Privacy concern was one of the concerns in the NOMA which has been investigated by Satrya and Shin (2017). It was claimed that iterative separation by SIC has the capacity can enable the harmful user so that the private messages can be extracted which had already been addressed to other designated user. The solution for the proposal included the importance of two keys which should be used in order to get rid of the problem. It means that one key should be used for the hashing whereas the other key should be used only for authentication. The first key will be responsible for making sure that the legal user is performing whereas the second key consists the embodiment of the MAC and IMEI of the user's.

# 2.9 Cognitive radio (CR) networks

In order to augment the performance of the radio spectrum, Cognitive Radio (CR) can play a crucial role in that regard that is learnt from Soliman et al (2017).




It is responsible for making a bridge between the licensed and unlicensed users so that they can coexist by utilizing various spectrums. Licensed users possess a higher degree of priority and also are regarded as primary users. On the other hand, the unlicensed users are regarded as the secondary users and they can have the transmission only when the spectrum possesses a hole which was left off by the primary users. Software Defined Radio (SDR) can provide the way of achieving the spectrum-sensing radio since this is way more convenient for the users (Soliman, et al, 2017). This particular technology possesses the improvement in capacity as well as throughput rate. However, the complex operation of this technology lets itself towards vulnerable attack (Soliman, et al, 2017). .There are solutions which have been proposed such as the usage of PLS solution for the protocols regarding transmission in the CR Networks (CRN).High risk persists on the primary user due to the coexistence of both primary and secondary user where the chance of eavesdropping is not minimal (xei, et al , 2017). To provide solution for this subject matter, Xie et al. has come up with an idea that states of the addition of noise in the signal through the Superimposed Coding (SC) so that the original signal can experience the interference; hence the primary user's concern of privacy on eavesdropping can be taken care of.

## 2.10 The security aspect of 5G in vehicle to everything

The paper from Bian et al. (2017) depicts the aspects of security in relation to the V2X communication system. They came up with different types of challenges which could not be taken care of by the given standards such as platoon disruption attack which was found on the basis of old packets, data falsification attack by providing false pictures or videos. On another note, it is almost impossible to find the jamming attacks. These issues can be taken care of by introducing non-cryptographic security mechanisms in this regard. The example can be given on a car of a specific platoon which could be responsible for collecting data from different vehicles so that it could be understood if there was any deviation such as statistical interference. In order to get rid of jamming, it is important to set up a channel hopping process so that the communicating parties can hop on through a sequential process which is completely exotic to the attacker. One of the most challenging sides of the non-cryptographic mechanisms is the delay that actually concerns the parties (Eiza ,et al , 2016).

## 2.11 security aspects of 5G over the physical layer

There have been many investigations that lead towards doing research on the wireless physical layer security in 5G. Two layers have been identified by the researchers which are known as physical layer authentication and Physical Layer Security (PLS). According to Sun and Du, (2017) PLS has the application which is suitable for use in 5G confidentiality. PLS can have the artificial injection of noise that can decrease the quality of the channel; hence, the channel quality of the receiver-end remains good. Studies have revealed that cryptographic approaches are less fast in terms of key distribution than PLS technology. In addition to that, unlike the solutions and services that cryptographic approaches serve, PLS is capable of providing higher security levels. The new offerings of 5G may not go hand-in-hand with the current technology of PLS; therefore, a solution has been proposed so that the PLS technology can better fit with the features of 5G according to Sun and Du (2017). In case for the ultra-low latency, it is imperative to use PLS on the basis where the eavesdropper might not be able to get what he/she intends to get in the given time. That is why Farhang et al. (2015) proposed physical layer security which can ensure the protection from the vulnerability in 5G NR. The access points are comparatively smaller and that actually can play a part in disclosing the location. However, the location can be disclosed with pinpoint accuracy and authors have proposed an interesting solution by formulating a mechanism to use the ‘noise’ at

the access point. The same thing has been found by Yu et al. (2016) proposing a solution through the distribution of knowledge.

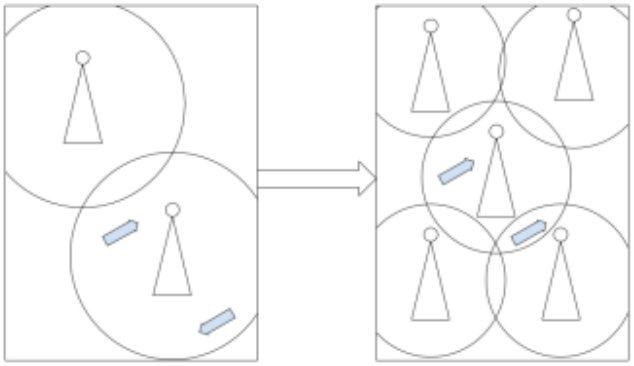


**Figure 2.5:** In 5G, there will be more base stations with smaller cells. The arrows symbolize connected vehicles.

Pan et al. (2015) have come up with the physical layer authentication which is devised on the basis of the channel response and is unique in nature. The response of the channel can be used as a means of fingerprint because of the uniqueness of the features. This has also been investigated by Xieet al.(2017) for authentication of the symmetric key in the distribution process.

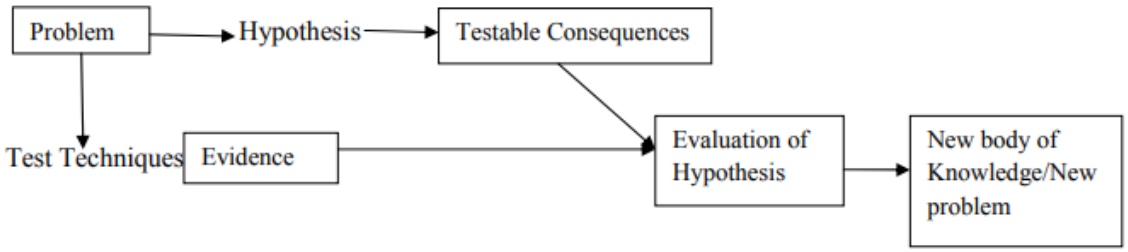
# 3

# 3 Research Methodology

## Introduction:

The research methodology is a vital chapter of a research thesis paper. It is a go through the theoretical and systemic analysis that has been applied for the purpose of the research.

To select and implement a specific methodology is of very important because it helps in data collection on the ground of literature and facts. Irny and Rose ( 2005) used a method for researching. The below-mentioned flow chart shows how a researcher can go through until they reach a certain result.

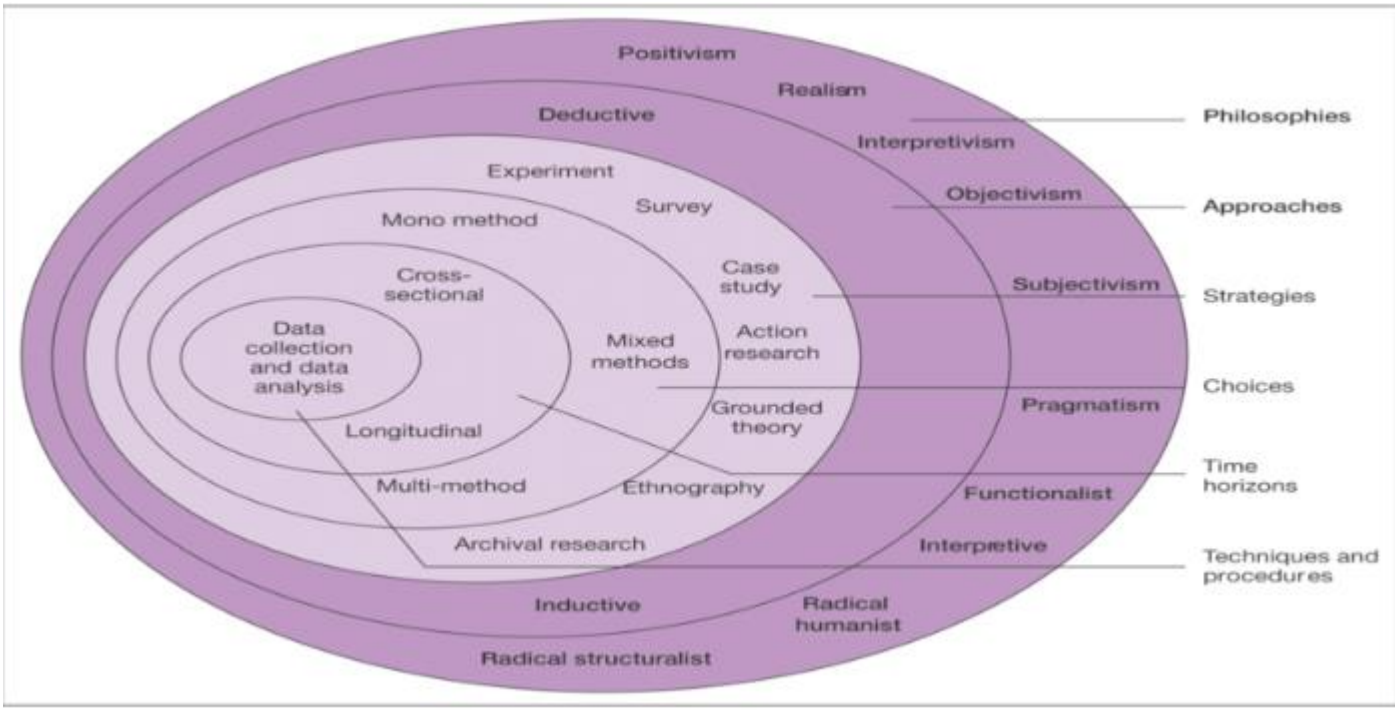



It makes the process simpler and helps observe new facts and draw conclusions. There are different types of research methodologies. And that differs depending on the research type and criteria. we are mostly focusing on the Descriptive research where we collect data from the different resources and other papers. In methodology, we briefly describe how we have collected data, how the research questions have solved or how we have tried to get to the solution for a problem.

## 3.1 Research Philosophy

There are several options to choose from with respect to the data collection system which can be based on the research topic or the research arena. Hence, it is a must for a researcher to follow a certain course of action to conduct the research. Though there have been different choices of modes given in the (Saunders , et al., 2009) book, a handful of choice has been made with respect to the need of this study.

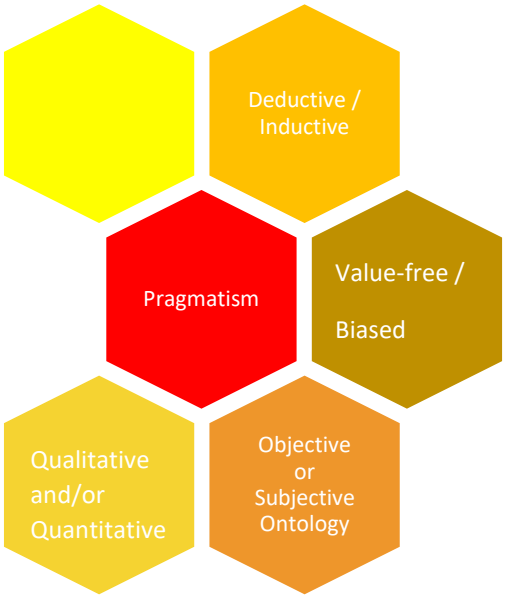
It is necessary to have a discussion on the Research Onion before going into the details.




The research onion portrays the step-by-step process of the research which entails the activities the research does and the views that the researcher holds. It is mandatory to go for in-depth analysis and the layers of the onion should be done thoroughly up until the desired outcome of the research.

Saunders (2009) had come up with four philosophies on the research which would let the researchers utilize one philosophy that is the amalgamation of two philosophies technically. ***Pragmatic*** research philosophy depicts the research process in a multi-dimensional way and interprets the process of that research. In addition, the data have the inclusion of two important paradigms which are called interpretivism and positivism (Saunders , et al., 2009). The positivist research paradigm relies on the collection of data whereas the interpretation focuses on the source of the gathered data. In addition, interpretivism research paradigm can pave way to analysis further so that a possible solution can be achieved (Saunders , et al., 2009).

The following figure discusses the factual data with respect to the pragmatism:

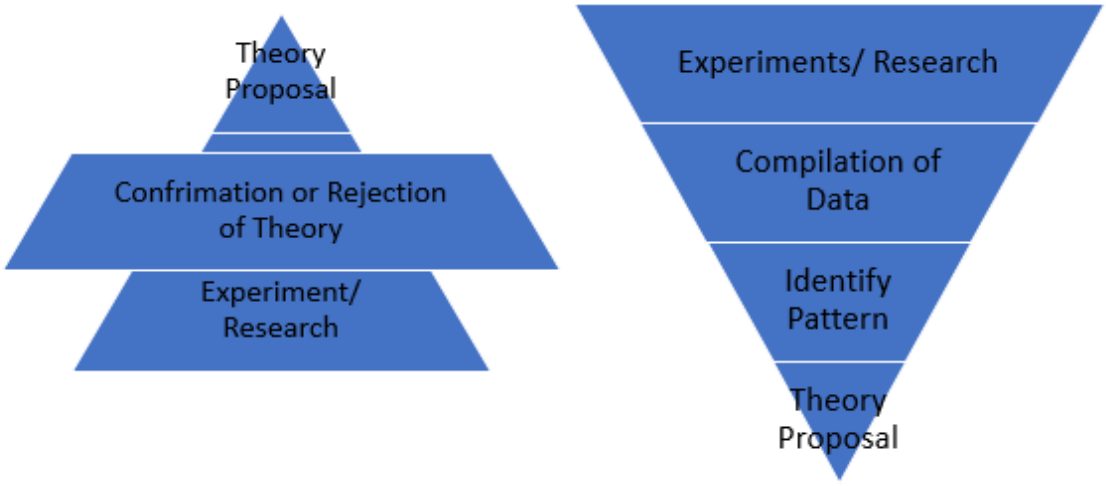



The analysis of the paradigms certainly depicts the philosophy of pragmatism. That being said, the observation will increase the validity of this approach with a view to collecting data as well as interpreting different techniques.

# 3.2 Research Approach

Two kinds of approaches are applied for reasoning that can emphasize on many parts of a research. One is the inductive approach and the other is a deductive approach (Trochim, 2006). The first one is a process which takes a step from a very specific perspective to a general perspective. On the other hand, deduction is a process that works with a general viewpoint and gradually moves toward a specific one. Deductive researchers usually begin their process using a formation which is like a 'top down' manner (Creswell &Clark, 2007).

Hence, the deductive approach can be summed up with a top-down approach and this needs to possess a theory which is needed to have proof to accept whereas the inductive approach is can be represented by bottom-up approach (Saunders , et al., 2009).




But when it comes to the inductive research process, the researchers tend to work from the bottom to the top while working on the opinions of the respondents with a view to creating a wide array of themes and generating them according to the theory (Creswell & Clark, 2007). More specifically, the approaches mentioned before have similarities with quantitative and qualitative methods, which are also known as deductive method and inductive method respectively. But not every researcher supports the combination of inductive-deductive or quantitative-qualitative. So it is prudent to treat each of them differently.

The collection and organization of data will be based on the survey, interview, literature reviews, and questionnaires. Afterwards, the organized data will be utilized to identify the aspects of this research which can enable the researcher to deduce the main purpose of this research on the basis of smart vehicular transportation system.

## 3.3 Research Strategy

There are numerous strategies that are undertaken by the researchers which suit their research topics such as the grounded theory, survey, ethnographic strategy, experiment research, action research, and combination of action and experiment research. It is needed to justify the mode of research strategy so that the researchers can move forward with the research strategy (Bernard, 2011). However, time can be the essence of research and there are strategies that consume huge time to cover. This is why survey can be designed to collect primary data from the respondents and this is not very time consuming provided that the respondents are ample in number (Saunders , et al., 2009).

This study requires collecting data from the respondents who heavily use transportation to go from one place to another frequently. Hence, it would not be wise to interview all the people and also, it would consume huge time as well. Research strategies like action research, archival research or grounded theory would not be suitable for the Vehicle to vehicle communication over 5G network since not much

information can be found on the internet due to being a modern concept. That is why going for the survey would be the right fit for the research to inject awareness to the people for the security concern and to collect the insights from the respondents on their needs.

# 3.4 Data Collection Methods

In case of primary data collection method, the difference can be understood by the data collection type where one type is mostly based on the numerical data whereas the other type represents the exploratory nature of the research (McCusker & Gunaydin, 2015). The quantitative research concentrates on the statistical data and is densely used by researchers since it can provide exact information of what the researchers are actually looking for. On the other hand, qualitative research focuses on attitudes as well as different correspondents and experiences to shed light on the research topic.

| Steps in the Process of Research | Quantitative | Qualitative |
|---|---|---|
| **Research Problem** | Definition, Detail and Evidence | Examination and Perception |
| **Review of Related Literatures** | -Major Importance | -Minor Importance |
| **Specifying a purpose** | -Specified yet quantifiable and observable | -General and broad |
| **Collecting the data** | -Numeric data<br>-Large population sample | -Text or image data<br>-Small number of individuals or sites<br>- Participants' experiences, culture, attitude etc. |
| **Data Analysis and Interpretation** | -Statistical analysis<br>-Relationship of trends and comparison of groups<br>-Results may vary from past data being used as determinants for predictions | -Essay analysis<br>-Descriptive Analysis "Reading in between lines"<br>-Overall understanding |
| **Data Quality Determination** | -Reliable and Valid | -Verification and not internal validity<br>-Transferability and not generalizability<br>-Confirmation of findings |
| **Research Presentation** | -Standard and unbiased | -Flexible, Emerging, Reflexive and Biased |

### 3.4.1 Interview

In an interview, data is collected by the researcher who asks a respondent certain questions and the respondent answers them accordingly. In the case of the consultancy of an expert, an interview is considered very important because the expert can enrich the interview with valuable insights.. The obtained data is of high quality as it comes from the experiences of the respondent. In addition to this, the related cost of collecting data by arranging interviews is higher than other methods of data collection (Odoh and Chinedum E, 2014).

In our purpose for research, we have conducted interviews with our fellow students and some of the cybersecurity experts from Oxford University and chamber university Sweden (appendix V and VI). The interviews had help us come up with the different research questions. As the interview was between the Field known personals the questions were technical. We have conducted some of the researchers around the world who are working on this topic, we sent them interview questions and ask them if they could possibly answer them on their time.

One of the researchers from Sweden has replied with the very In-depth answerers over the skype and it helped us to analyze our data. Piers O'Hanlon from oxford university had participated in an interview. We have benefited from that interview as well. In appendix VI we have attached the interview transcript.

### 3.4.2 Questionnaire

Another easy method of collecting data is questionnaire. It represents the respondents' observations by asking them a set of questions where they express their thoughts and opinions regarding that certain phenomenon. When the questionnaire is made according to the standard, respondents will be willingly provide their insights about the topic. Then and only then the questionnaire will be able to contain their attitudes. But for that, the questionnaire has to be well structured. It will be given to the respondents and they will have to fill it up according to their thoughts and beliefs (Odoh and Chinedum E, 2014). The questionnaire has to be free from bias and cannot contain anything that makes the respondents unwilling to answer. Distributing the questionnaire to the respondents is not an easy job to do. The respondents may live in different places. In that case, the questionnaire can be mailed them via online or offline or both systems. Additionally, telephone communication can be used in this regard but that may make the respondents uncomfortable if the situation comes where they have something to say that does not

support the related company or the person doing the research (Odoh and Chinedum E, 2014). This is the reason why a questionnaire should be made with proper guidelines so that it can be a useful method of the survey research.

Interviews of prominent researchers and associated personnel have been taken from different sources and this has provided important input in coming up with the prospects of 5G network with respect to the vehicular cellular network technology.

As we have chosen to conduct interview in our case we have included the questions we have asked to the researchers.

The topic of interest was consisted with but not limited to :

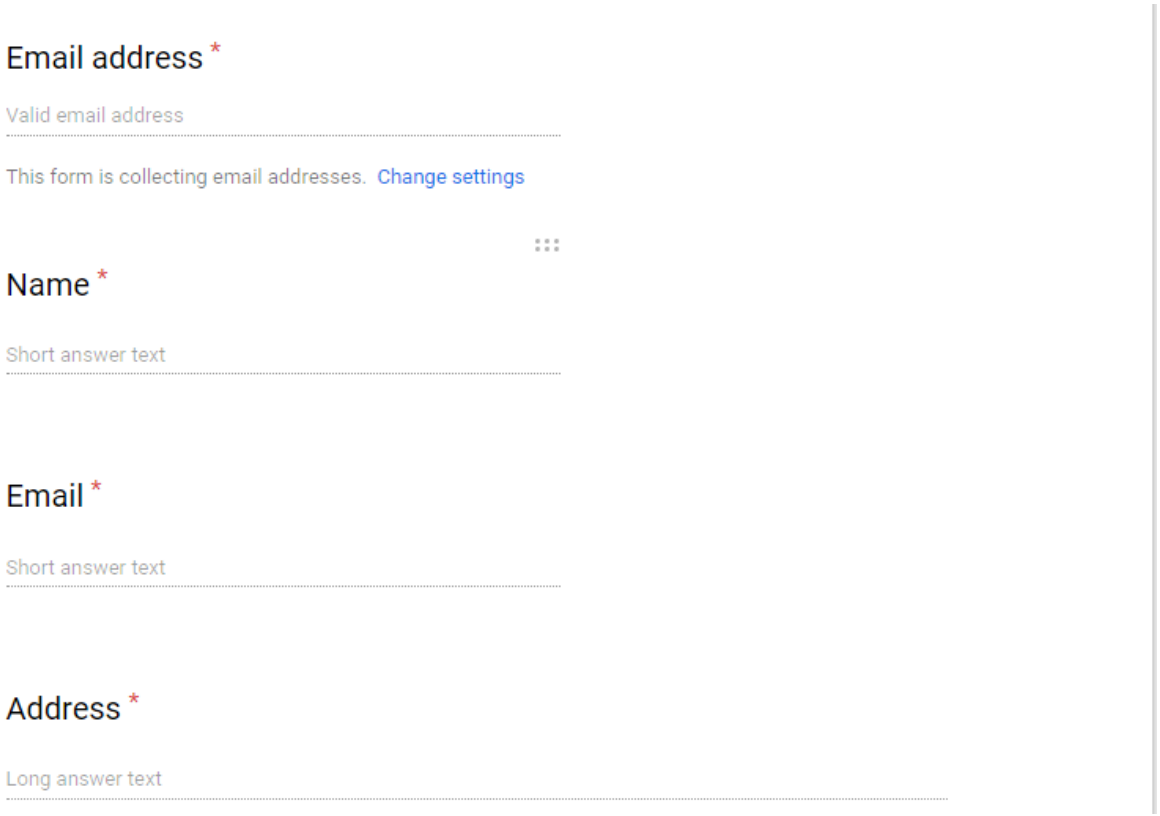
- Verification establishment for the vehicular networks.
- Access authentication for autonomous Vehicular net.
- Attack resistancy
- Requirements for the ITS
- Security in ETSI v2X communication
- CIA triad model in the V2X network

### 3.4.3 Survey

Conducting survey is a part of primary research. In our case we had used the case study as our research strategy. But we also have taken some secondary survey data that has been conducted by other researchers. This type of research works as a medium that helps understand others' perceptions and analyze them to know more about a specific occurrence.

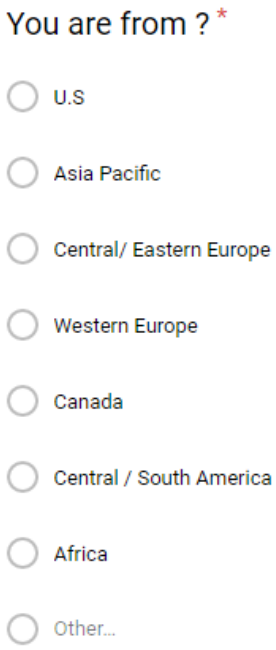
The implementation and capacity of a survey technique cannot be restricted to a single area because of the characteristics of that technique. Survey is one of the most used techniques and to conduct it requires a lot of apprehensions. Survey can be used properly to understand the perspectives of the respondents. It can uphold the present scenario regarding the research topic. For this, survey is the most popular method of data collection (Odoh and Chinedum, 2014).

### *3.4.3.1 Basic information*



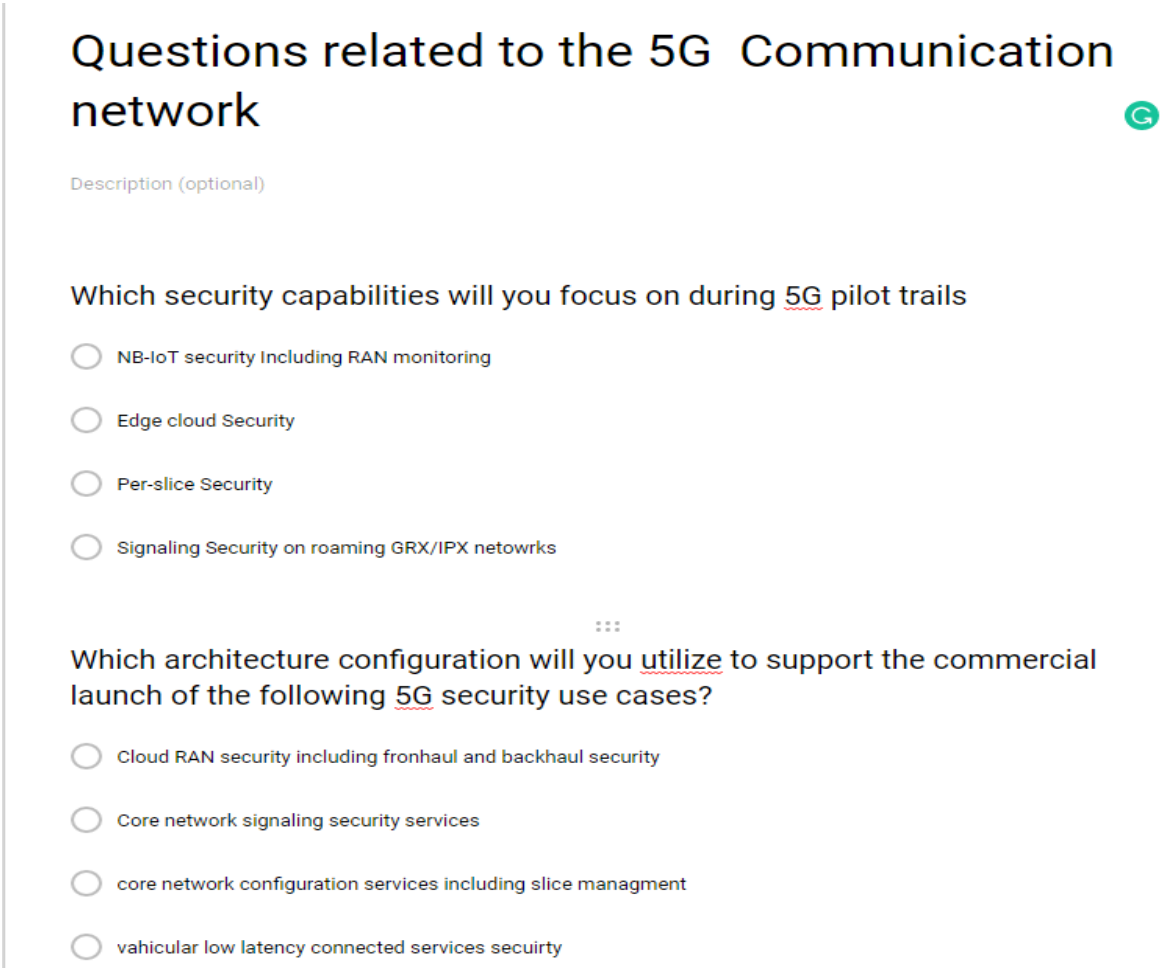

It is necessary to have the demographic information to do the survey and this is why the basic information has been asked from the respondents with a view to having a knowledge on their responses.

### *3.4.3.2 Origin*




The aforementioned information is necessary to know. Since vehicular network only persists in developed countries, the continents/countries of the respondents can play a vital role in determining the responses.

### *3.4.3.3 Main part of survey*




All the questions will be needed to respond to the respondents. The analysis will be avidly discussed in the analysis chapter whereas the questionnaire will be kept in the appendix for further references.

## 3.5 Data Analysis Methods

The visual representation will be undertaken through using pie charts, bar graphs, and line graphs which will portray the relationship among different variables. Later, the data presentations will include the descriptive analysis so that the findings of the research can be disclosed and interpreted accordingly.

## 3.6 Ethical Consideration

According to the Ethics documentation of Northumbria University, no boundary persists in the ethical practice, problems, and principles. It is compulsory for all the students to participate in the research so that they can practice of being ethical and punctual while they are engaged in the research work (Northumbria

University, 2018). In addition, the research ethics committee has been successful in eradicating all sorts of ethical dilemma which is one of the most important factors according to (Saunders , et al., 2009). Privacy of the respondents should be given top priority when respondents agree to participate in the survey (Saunders , et al., 2009). In addition, the respondents cannot be forced to participate either and they will be expected to participate voluntarily. Also, the respondents should find no discomfort in participating in the survey and they should not expect any biasness in the questionnaire. That being said, the wording of the questionnaire should be poised in a way that cannot create any negativity in the mind of the respondents (Saunders , et al., 2009). Therefore, the respondents are entitled to have a choice of not giving out the personal information stated by the General Data Protection Regulation (Information Commisioner's Office, 2019).

# 4

# 4 Research Analysis

## Introduction:

In prior sections of this study, this research paper had already discussed the impact of 5G radio technologies in V2X communication and how it can provide protection to the existing system. In this section, the data analysis will take place as the data collected from the respondents had already been taken. It is important to mention that the data analysis will be able to answer the research questions.

## 4.1 Literature Review analysis based on our research questions

In this section, the insights from extensive literature review had been taken and explained to find out the answers of the research questions posed at the beginning of the research. The analysis will be done on the basis of CIA triad. That will ensure the maintenance of the security and also the goal of this research will be achieved.

The questions are as follows:

- RQ1: What type of security mechanisms and protocols has been considered in ETSI V2X communications till now?
- RQ2: What type of security requirements are needed for several use cases of ETSI ITS?
- RQ3: What are the features that can be utilized at the physical layer in order to develop the security measures of 5G? Is it possible to repudiate any security mechanism from the higher layer protocols?
- RQ4: What are the vulnerabilities that 5G NR can cause to V2X communication?
- RQ5: Will it be possible to replace 802.11p with 5G NR? What are the stymies if it is not possible to replace?

Security stands for the protection for the important information to control the accessibility of the unauthorized personnel. It actually has a combination of Confidentiality, Integrity, and Availability.

In the following, the research questions will be addressed and answered accordingly with the assistance of literature reviews and analysis of the survey responses.

### 4.1.1 RQ1: security mechanisms and protocols in ETSI V2X communications

According to section 2.1, this particular question has already been answered and explained in full. Findings will be summarized here in this part and the security mechanism that has been used in the ETSI ITS will be explained in brief in the following. The packet of SecuredMessage is a combination of different types of payloads that are DENM or CAM in nature. Also, these are the requirements that the security layer needs for the various types of trailers as well as headers. The SecuredMessage header carries a unique version protocol and also the security profile. In order to portray the format of the messages such as payload, compulsory header, and trailer fields, the security profile is used. In addition, it was also used in terms of encoding. In case of **confidentiality**, CAMS and DENMs have stated that no messages should be encrypted as per the security profile for the CAMs and DENMs (European Telecommunications Standards Institute,2013) As the research moves towards the following sections, the confidentiality of data can merely be regarded as a problem in applications for the basic sets. At the time of **authentication** of any user through a certificate authority, a public key is being used for exchanging the credentials cryptographically (European Telecommunications Standards Institute,2010). On the other hand, authentication, as well as **integrity** in ETSI ITS model experience the cryptographic signatures so that the authentication of the sender can be done as well as the integrity of the messages, can be guaranteed (European Telecommunications Standards Institute,2010).The message is verified as well as signed by using asymmetric cryptography or symmetric cryptography. **Privacy** is guaranteed for the sender since the user cannot be tracked down. Hence, the pseudonyms are needed to possess updates every now and then (European Telecommunications Standards Institute,2012). In addition, for the attacker, it is very difficult and close to impossible to establish a connection or a link of the pseudonym to canonical identity of the users (European Telecommunications Standards Institute,2010). In terms of **availability**, there are no such guarantees that have been found which can explain the ETSI ITS security documents. According to (European Telecommunications Standards Institute,2010), availability has already been taken into account along with the solutions. Some of these have inclusion of “Include the origin address in every V2V message”, “Limitation of all message traffic to the V2I/I2V and the places where it is suitable”, and “Include a sequential number in new message”. It is one of the requirements for the certificate structure to provide the validation as well as the distribution of the asymmetric keys so that the encryption and the signatures can be done. Granting the certificates is a responsibility for the Certificate Authorities (CAs) who does the work by maintaining a hierarchy. On top of everything, ‘ultimate root of trust’ lies and it is called the Root CA whereas the down livings are called the Authorization CA and the Enrollment CA. The responsibility of the Enrolment CA has inclusion of the initial authentication and also it is responsible for

providing pseudonym to users. Afterwards, the Authorization CA provides the users with permission in accordance with their needs so that the users can perform their operations accordingly.

### 4.1.2 RQ2: security requirements are needed for several use cases of ETSI ITS

**Availability:** The class of this application has very rigorous requirements on availability since the concern over safety is regarded as one of the highest priorities to be delivered.

**Confidentiality:** Confidentiality is not very much important because the warnings are delivered to the ones who might be vulnerable to the upcoming danger.

**Integrity:** In terms of safety measures, integrity is vital to be acknowledged. A fabricated message has the potential to divert the operation in a wrong way. For example, if a vehicle sends a warning on the 'slow vehicle', it should mean that only. However, if it is modified and meant something which was not very urgent, like a Point of Interest notification, this might lead towards causing havoc in the road.

**Authentication:** Authentication can vary from numerous use cases. In case for warning messages, this is only a requirement by the receiving transports for the identification of the location. With respect to the receiving end, no actual need of the identity persists because of the authenticity of the users' location and the delivery of the messages. On the contrary, for audit purposes, it might have used so that the identification can be done for the misbehaving users. However, it is possible to falsify the identification. The attacker can send a fabricated warning for an accident. The receiver will be able to notice that the sender possesses another location through the location authentication. That is why, it is not important for the full authentication. Nevertheless, for special vehicles, it is imperative to have authentication such as the emergency vehicle warning system for the emergency vehicle.

**Privacy:** The privacy concern is very important in this respect and the requirements can vary at times. Privacy is very important in terms of providing protection and security for the slow vehicle indication, emergency vehicle warning, co-operative glare reduction, and motorcycle approaching indication since these are the most used messages that are being delivered during the trip. In case of a collision warning, a privacy risk may arise. Privacy might seem to be problematic for the lane change warning and overtaking vehicle warning provided that the user frequently overtakes and changes lane. These cases comprise road hazards warnings and these have no potential threat to track the users.

### 4.1.3 RQ3: security measures of 5G in NR or New radio frequency

Except for the emergency vehicle warning, authentication is highly required for the receivers to locate the location of the sender. Meanwhile, it is important to have the identity for the authorities so that they can always remain in the business of tracking misbehaving users.

**Physical layer authentication:** In the physical layer, location authentication can take place by utilizing the physical layer authentication technology which has already been discussed in the subsections 2.11 and 2.6. In addition, beamforming technology can augment technology and has the potential to make life difficult for the attacker to anticipate the location-dependent channel signature. In addition, it can provide better performance for the collision risk warning. But, this technology is not suitable for the decentralized floating car data due to the fact that the sender is not needed to stay at a particular place.

**Availability through NOMA and cognitive radio**: In general, for any road safety cases, availability is a must for all the cases. A special risk is found in the decentralized floating car for availability. The messages are being repeated for numerous times from a particular time to another car and an attacker has the potential to multiply the messages and turn the messages into 'waves'. As a result, a message flood can be experienced which eventually jam network and consequently, the users will lose access to the network. This is why it is imperative to install mechanisms that can work as a shield to encounter the attacks. Cognitive radio network, as well as NOMA scheduling, can provide availability upon being utilized. In addition, as per the subsections of 2.8 and 2.9, these technologies have the capability to utilize resources inefficient manner for the availability of the network.

### 4.1.4 RQ4: vulnerabilities that 5G NR can cause to V2X communication

**Vulnerabilities**: Some security requirements can be solved by the new security solutions provided in the prior sections. However, the 5G NR is prone to vulnerable security analysts which mean the OEMs should be on its feet to tackle the vulnerabilities efficiently. The following parts will provide solutions which have been discovered from the responses of the respondents.

**Privacy:** New technologies germane to the 5G NR have been discussed in this paper and it had identified that privacy can be a concern in this case. The location of the user can be known by introducing small cells which force mmWave to work for the attacker. According to section 2.11, this can be prevented by doing randomization of the base. In section 2.6, it has been discussed that privacy can be an issue in case of using beamforming technology since this requires the implication of tracking the location of the user. NOMA can originate privacy concerns since the receiver is responsible for extraction of the strongest signals with different destinations which have been discussed in 2.8.

**Availability:** Availability problems can be found in the cognitive radio since the operation is complex according to section 2.9 Proposed methods in that section can ease the complications of the cognitive radio.

**Confidentiality:** Confidentiality can be a concern in the cognitive radio. Therefore, numerous authors have studied and come up with numerous solutions on confidentiality issues in the cognitive radio which has

been discussed avidly in section 2.9, One of the solutions revealed that the introduction of noise to the eavesdroppers. In the meantime, the channel between the receiver and the sender remains unharmed. This method is identical to the PLS.

### 4.1.5 RQ5: Possible Exchange 802.11p with 5G NR

A research question, in the beginning, had been formulated to see whether the replacement of 802.11p along with the 5G NR might be completed. To be able to answer that, it is needed to acknowledge that it is possible to work simultaneously. However, the NR has not been defined and it is possible to improve it according to the needs. Because of the modularity network stack, the change of scheduling method (NOMA) or frequency transmission should not be able to put any impact on higher layer protocols in this regard. According to the subsection 2.3, the 5G NR is regarded as the developing technology; hence, it will not be a wise decision to compare this with the IEEE 802.11p protocols which lay in ETSI ITS model. However, the 802.11p protocol can be compared to C-V2X. In another subsection 2.3, a table has been formulated to provide a clear view of the features of the aforementioned technologies. The C-V2X and the 802.11p possess almost identical feature whereas the differences have been noted in table 3.2 that represented the usefulness and the stymies of taking C-V2X in lieu 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

According to the table, the stymies of the C-V2X can possess a serious threat to the benefits. Having said that, the problems have already been solved the problems in 5G V2X. In addition, the Doppler Effect has also been taken into account and also been solved since this effect can become problematic in the time when the vehicles move fast. This actually represents the connection of both LTE and 5G NR base station (Qualcomm. Designing 5G NR, 2018)

**Redundant cryptographic mechanisms**

The aforementioned subscriptions have been portraying every aspect of the security concern. The security concern of the use cases is the integrity, availability, and authentication. In addition, it has also been understood from the discussion that the physical layer technologies can extend the assistance to give necessary solutions in this regard. The receiver needs the authentication of the location and this is exactly where the cryptographic signatures can prove to be redundant in the use cases. However, this problem can be taken into action by channelling the signatures. In addition, the encryption is not needed for the selected use cases. Cryptographic authentication can be amalgamated with the physical layer authentication so that full authentication can be achieved in terms of identity and location [72], [15]. That being said, it is evident that the certificate infrastructure, as well as the cryptographic keys, is the ones which are greatly needed in some of the particular cases. It is done when the authority wants to track the users who have been behaving in a different way that they should not be. If IBC can be embraced for the vehicular system, the certificate infrastructure can go towards being redundant. The prior sections had gone through discussing the IBC with respect to the IoT. However, it is necessary to have adjustments for the V2X. Needless to say, this technology has the potential to become one of the most important technologies in the future that can ensure the optimization of the cryptographic mechanisms. Thus, it is an essential sector to divulge the resources in it.

**Other 5G security technologies**

Since the prior subsections advised, integrity, as well as authentication, can have a solution to small extent if the channel signatures are being used. That being said, the case that it is being dealt with in this thesis does require availability with respect to the emergency vehicle warning. The subsection possesses security solutions for all the requirements. In addition to that, some solutions have been provided for the requirements.

**Availability:** Availability holds the possibility to be solved in an implicit manner. There are numerous methods which can develop the availability to a newer extent. Bian et al. [20] have come up with a solution by installing channel which can be established in order to get rid of jamming. The parties can hop on in between the channels through a particular sequence which is completely unknown to the attacker (see Subsection 2.10). The different solutions have inclusion of packet

forwarding approach so that the message storms and flooding can be gotten rid of which has been initiated by the broadcasts.

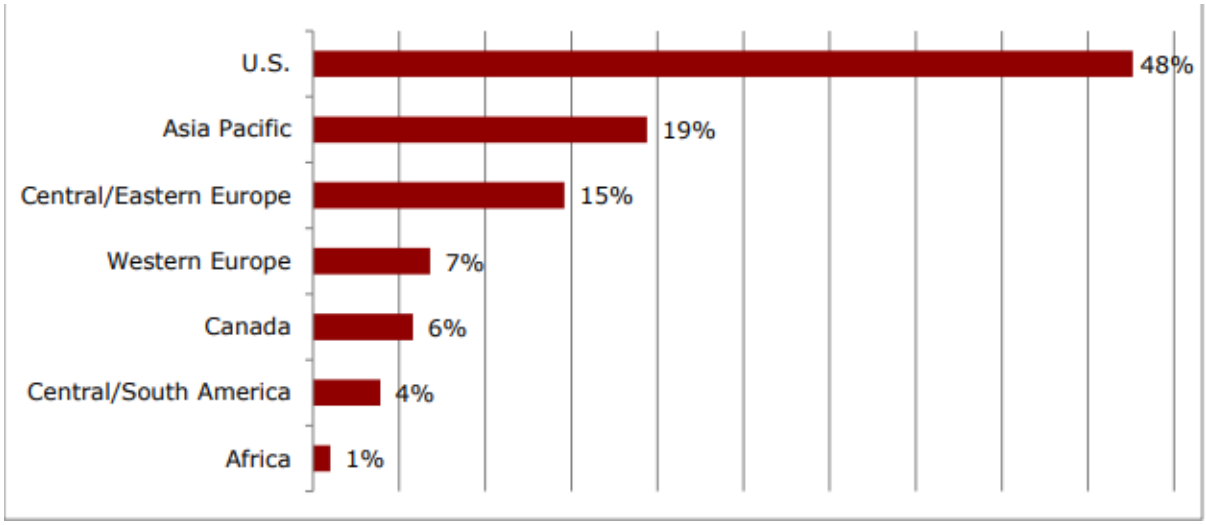
**Privacy:** Privacy cannot be considered as a vital element for the use cases. However, by randomizing the choice on the basis of the base station, it can be solved to some extent which has been discussed in Farhang et al. (see Subsection 2.11).

**Confidentiality:** There have been various methods which can be appropriate in solving confidentiality by having a go through the PLS (see Subsection 2.11). However, in the use cases, confidentiality has no importance. This can be utilized in instant messaging, parking management or automatic access control system.

**Authentication:** 5G core network can have application if the vehicle resided inside the network. The 5G-AKA protocol (see Subsection in use case one;4.3.1) can easily be used for UE which has a USIM that can communicate with the base station. 5G technology has the potential and capability to authenticate users. It is important to find all the necessary information on the aforementioned technologies so that the efficient and effective one can be selected for V2X communication.

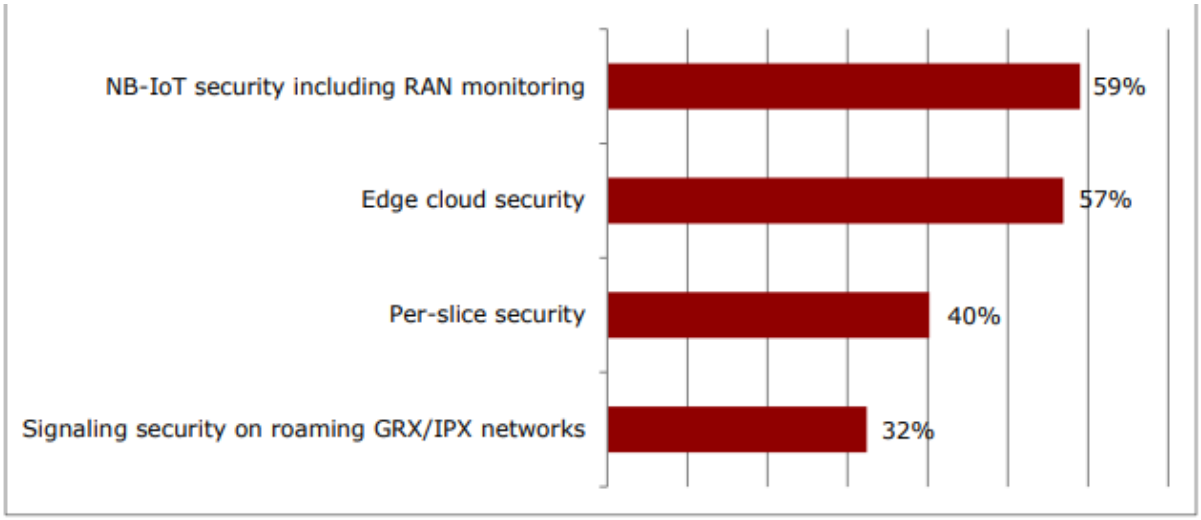
# 4.2 Data analysis of our survey

In the first part we are analyzing primary data that we have collected whilst we had done survey. We have conducted survey on "5G Security Survey" with some questions on internet. We have conducted the survey from around the world. In this part we are analyzing the data that we have collected from the survey in the 5G security prospective.



In this survey we got the response from the above graph that shows that the US people are more concern about the 5G security than any other countries in the world. And Africa the least country that are concerned and they have not many people have contributed in the survey.

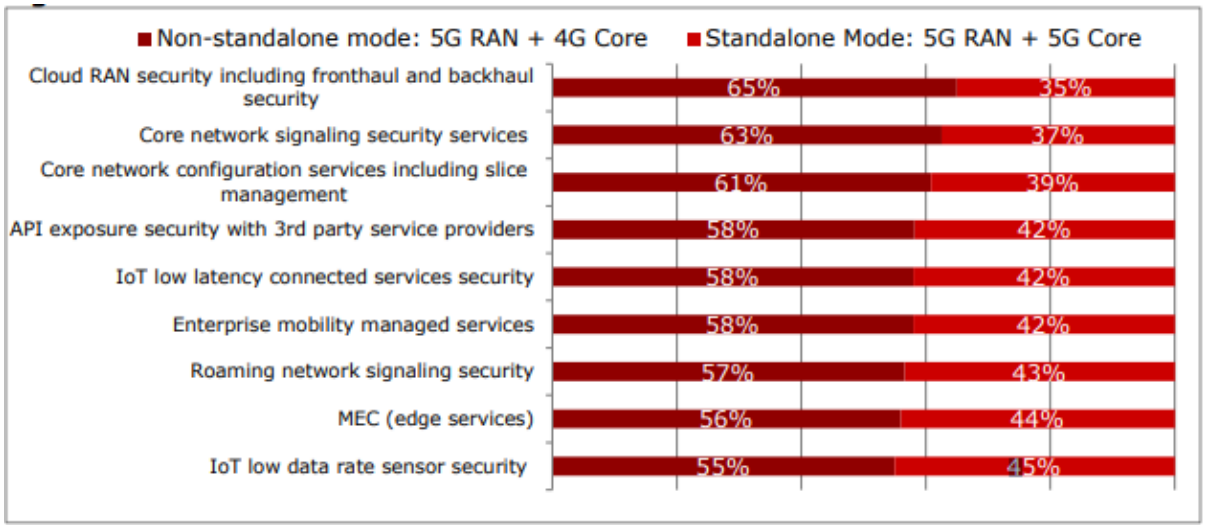
**There were a question** "What might be the concern you will have if you were to emphasise on trail program in term of security proficiencies"




The Radio structure that is fully scattered and have perfect control of users' plane by implementing 5G NGC and NR has a major concern implication.

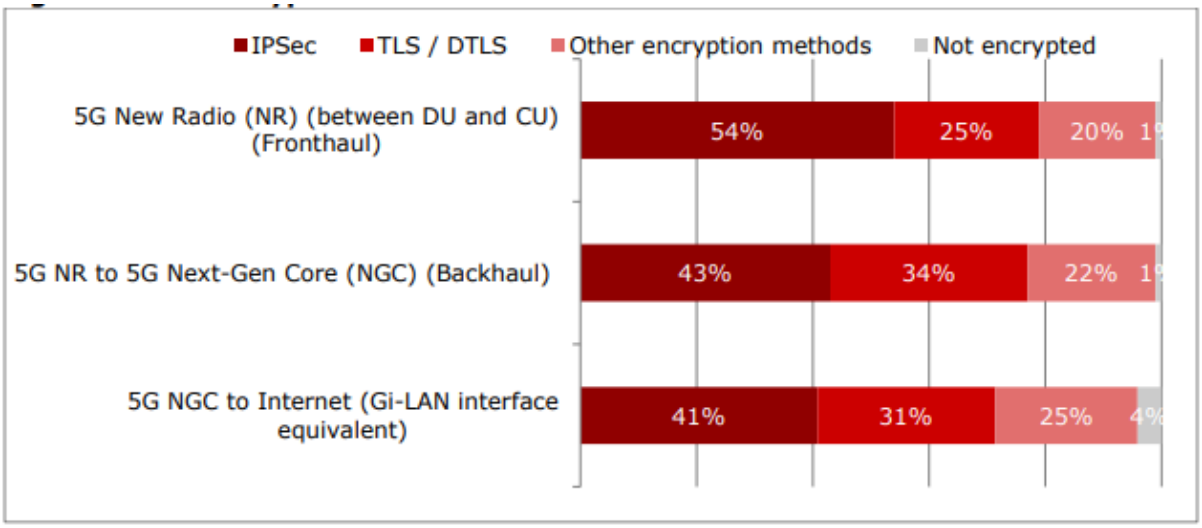
In the respond to that the CSP's had to come up with the solution that can provide a fulfilling security measures that consists of all aspects of security, for instance signaling security, business security, and more over IOT and MEC services

### 4.2.1 Question: "if you were to launch the 5G on commercial basis, what would be the architechural design you would follow to support your business?"



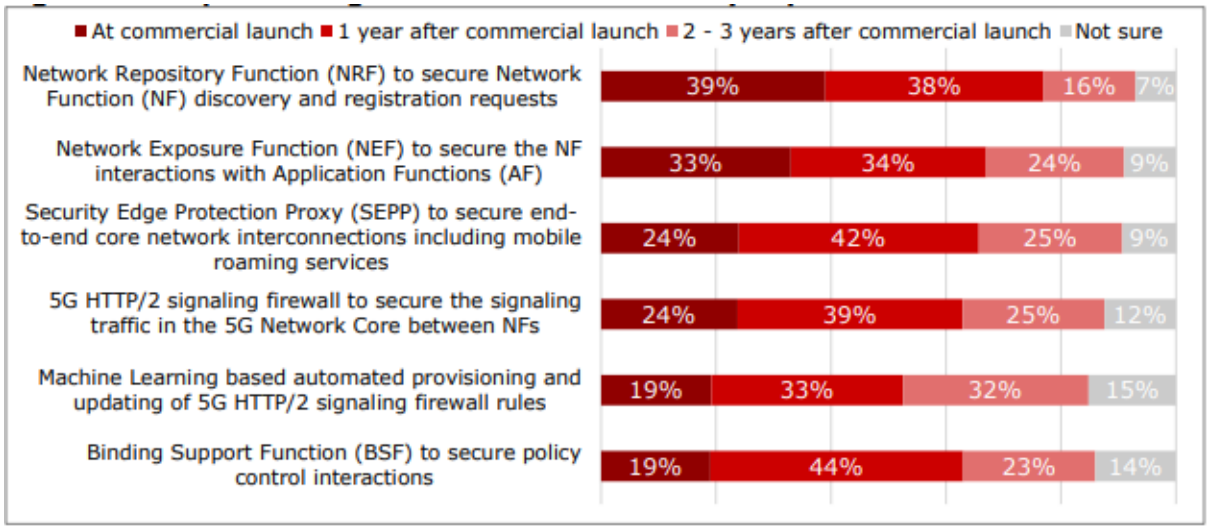
The strong focus is given on the cloud RAN security as well as core network signaling capacity which attracted 65% and 63% respectively. It is needed to be run in all configurations. This can also simplify the requirement to provide the support on the Internetwork Packet Exchange (IPX) so that the main core can have the usage in case for the launching operation. The NSA can easily pave the way for having less complexity for the security services.

### 4.2.2 Question: “can you tell us the what is the preferd encryption method you would chose for securing the users data in defferent layers? ”



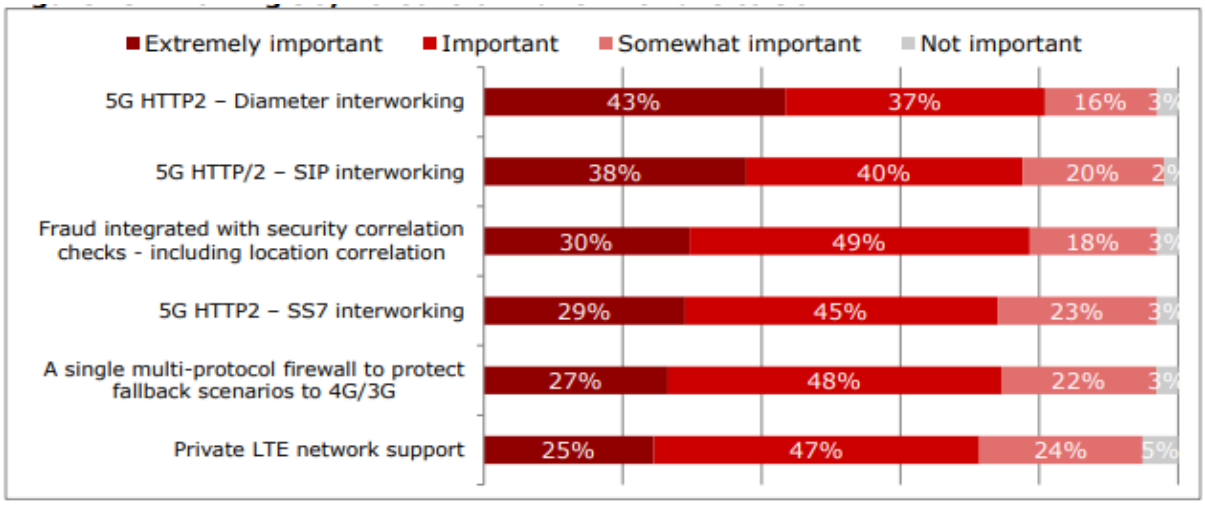

5G will be needed to provide the support for the encryption in a cloud-based architecture. Hence, it is a must to ace in comprehending the encryption preferences through different layers of networks for the end-to-end protocols for security. By having a close focus on RAN, the aforementioned figure possesses an impression of the radio network IPsec (54%) which is a type of encryption related to protocol based. In addition, there are other layers of networks which have also the preference on the IPsec. However, the support or the responses were put in 43% and 41& respectively. The usage of TLS protocol-based approach is the second preference selected by the respondents. The options have provided the support in the aforementioned boxes which had ranged from 25% to the RAN 34% which was done by facing to the core (known as backhaul interfaces) and 31% core which was done by facing internet. The Heavy Reading had the support of ‘other encryption methods’ and it had a range from 20% Ran to a maximum of 25% with respect to the internet-facing interface. Alternative protocol-based approaches can be used in terms of the QUIC which stands for Quick UDP Internet Connection which is responsible for the management of HTTP2 services in case of latent environment.

### 4.2.3 Question: “what would be time frame we are looking to implement the below mentioned control panel abilities in the security sector over 5g network”




According to the responses from the aforementioned figure, NRF is highly likeable among the respondents to be executed (39%) so that service profile delivery can be enabled. In addition, as a mode of commercial priority, the NEF is also capable of providing service (33%). However, in case for third place, a tie took place which were the SEPP (24%) for securing the roaming and the signaling of G firewall which is responsible for playing important role in securing signaling operation (24%).

### 4.2.4 Question: “Do you think that it is important to have the existing firewall (for 4G) for keeping the 5G network safe at the commercial market structure”



The challenges regarding the control plane of CSPs face is more like the management of complex as well as hybrid environment in order to make sure the uninterrupted working capacities of the protocols related to the 3G and 4G signaling. There lies an important consideration in the control for the 3G and 4G firewalls which have the capacity to support the 5G. In addition, this system can also be listed with all other attributes that have been mentioned in the questionnaire where 'extremely important' inputs had got attracted from HTTP2 – Diameter interworking (43%), HTTP2 – SIP interworking (38%), and then fraud/correlation capabilities (30%), HTTP2 – SS7 interworking (29%), and single/multiprotocol support firewall (27%), which reflects the need to support HTTP2 Diameter, SIP, and even SS7 interworking. The level of "important" responses (37% to 49%) is also significant. It reaffirms the focus on fraud/correlation (49%), single multiprotocol firewall (48%), and even the importance of private Long-Term Evolution (LTE) network support (47%), which continues to gain market traction.

# 4.3 Case study

Case study is another technique of research that compares the past condition and the current condition of a background to come up with a solution and take suggestions from that historical teaching in this third part we are discussing three case studies.

## 4.3.1 Case study one: 5G-AKA and ITS authentication

Arko et al (2017) published in there paper about the security and the efficiency. It is still up for debate about the efficiency of two technologies of authentication regarding the ITS model and 5G with respect to the V2X communication. For moving individuals, these technologies can provide assistance in utilizing limited resources and speed generation. In addition, it is needed to investigate about the 5G-AKA protocol which can be utilized for the users who are not inside the coverage.

On the other hand, the channel response is capable enough to provide fast and smooth authentication. The technology is not suitable for authenticating the sender through identifying the identifier. However, this can provide its services for re-authentication in warning messages to repeat simultaneously. It can be made possible if the authorities require no authentication for identity in delivered messages for audit. Before applying the technology, it is imperative to be able to put trust into and should be reliable as well as verified. In addition, the verification is needed to include the fingerprint along with the moving receivers and senders. The problems regarding security need to be acknowledged and checked in full so that serious caution can be taken to protect

the users from harmful things. Also, the beamforming can ensure the improvement of the physical layer authentication and later on, it can be added to ITS model. The integration should possess the cryptographic mechanisms and the physical layer authentication.

### 4.3.2 Case Study Two: Adapting IBC for V2X communications

Drias ,et al (2017) proposed IBC (Identity based cryptography), which is essential in order to repudiate the certificates that are needed in ITS model. This technology can ease the verification procedure for the keys and capable of authenticating directly so that no authority is needed to be contacted. If IBC can be integrated with the ITS, this will become one of the most important technologies which can perform better compared to 5G-AKA for V2X. IBC has a lot of promise to bring benefits; however, it is in deep need to adapt with the V2X communication. IoT is comparatively a look-alike of the V2X; hence, it is needless to say that IBC can be suitable for the V2X as well.

There are other modern technologies which can enhance the new possibilities for the 5G network to make it readily available. Cognitive radio (Soliman J. , et al , 2017) and NOMA (Kizilirmak, et al , 2016) scheduling are the two modern technologies that can really add value to the 5G. Cognitive radio is responsible for utilizing the resources in an efficient manner whereas NOMA scheduling is responsible for the transmission of different signals with identical frequency. If both of the aforementioned technologies can be integrated together, network availability will not be an issue. It is recommended to secure the execution procedure since NOMA scheduling has concerns over the security and the cognitive radio possesses a complicated nature which is vulnerable to the attackers.

### 4.3.3 Case Study three: Ericsson whitepaper

Ericsson (2018) had published a whitepaper on the security of 5G which states an abysmal view on the usage of various technologies in the 5G arena. The lists have inclusion of communication security, privacy, resilience, identity management, and security assurance. The communication security for both of the user plane traffic as well as signalling is kept in encryption. Also, the signalling traffic is generally protected. This can be available for user plane traffic. Privacy is a must in this case, and this is only provided by encrypting the identifier. This is a method for protection for the identifier, which is long term in nature and also, it is compulsory to refresh the identifier which is not permanent; thus, for short term purposes only. In case for resilience, isolation and separation method is taken into account. Identity management plays the same role as 4G does such as securing the cryptographic mechanisms, system for mutual verification

between the user and the network. In addition, this identity management is responsible for the portrait of EAP framework. The EAP framework is the best suited for mobile operators for the authentication purposes. The job of security assurance lies in ensuring the network so that the network can meet up the requirements to provide security. This is consisting of auditing infrastructure and requirements for security. In recent years, Oxford University published (2018)a report stating the technical vulnerability lies in the 5G-AKA protocol.

# 5

# 5 Recommendation and Conclusion

In this part of the thesis, light will be focused on the challenges which will be faced when the amalgamation will take place between 5G technology and V2X communication system. It is expected that this research topic will earn a lot of eyes to do research on. Future recommendations are given below based on the potential research challenges.

## 5.1 OPEN RESEARCH CHALLENGES AND FUTURE recommendations

- It is important to have found the latency which is limited to 1 millisecond at maximum level when the emergency situations take place. In addition, the automatic pilot in this case is very important which is needed to be on its toe to assist the driver as fast as it can do.
- It is important to consider the ultra-reliable communication system with respect to vehicle and to the safety for general public. Though there have been so many researches done in this sector, the connection between Internet of Things (IoT) and connected devices will surely make the issue into a complicated one.
- In addition to that, it is vital to have the research on the identification of different types of loopholes that might prove to be vulnerable for the communication system. Hence, it is compulsory to have huge work to be put on the physical layer so that the identification will be easier for the data and equipment. Another research challenge can be the usage of ML techniques which can efficiently analyse the abnormal behaviour of the attackers.
- In case for UAV operations, the main factors are reliability and latency and these factors are needed to be applied in the operation so that the assistance from the safeguard can be provided to the operation system. In addition, it is important to have a constant connection between the ground station and UAV for uninterrupted video streaming.
- In UAV communication, there are multiple problems related to the privacy as well as security which are needed to be taken care of. The problems are related to the spoofing, jamming, and eavesdropping. In order to provide solution for the problems, it is essential to follow AI solutions and lightweight techniques.

- Other challenges related to UAV communication can be the avoidance of collision as well as the fast and mobile support which have the potential to be researched on by the researchers.
- A reliable connection along with the high speed network is required for the monitoring processes. If not so, the researchers will not be able to possess exact and real-time data to make useful decision. However, getting high speed and a secured connection is a problem which is needed to be recovered by the researchers.
- It is necessary to provide support for the 3GPP SA3 security protocols and have an engagement with the system. In a given time period, it is important to become realistic and pragmatist whereas it is not expected to miss any opportunities to devise new things for the successful improvement of 5G.
- It is mandatory to provide encouragement to support the SDN/NFV security. In addition, the stimulation for the products are required that can provide support to the sensitive functionalities in different types of visualised environments.
- It is also advised to have proper communication with the Open source communities and also, it is needed to have the advocacy sp that it would bring more protection to the open source.
- The assurance of the security-by-default has been built in the developments of 5G/ It is also suggested by FCCG report that the security will be needed to have demonstration as part of the development program. The future research should also take into account the engagement of developers in the design of 5G test buds to have the establishment of security and protection in the initial stage.

# 5.2 Conclusion

5G itself is a recent phenomenon in this world and it is always making its way to make the lives better for the people. In addition, V2X communication has been there for a while to protect the secrecy of thousands and it has been one of the trusted modes of communications. This paper contains the study on the effect of 5G security focused on particularly vehicle to everything network, which can put a lot of impact on the security measurement of V2X communications. Literature study and participants' responses have been collected in order to analyse the impact of V2X communications upon the introduction of 5G technology. In the beginning, a model has been adopted, namely ETSI ITS model, with a view to describing the current status as well as standards for V2X communications. The security procedure and prospects have been portrayed in full. Later on, the solutions of the security problems have been discussed with respect to the 5G. The analysis part of this report depicts the security requirements on various use cases. In addition to that, there were corresponding solutions which were given based on the requirements. The investigation on the security aspects had inclusion of different variables germane to the authentication, privacy,

confidentiality, availability and integrity of the system. In the research, it was discovered that the 5G-AKA protocol as well as the physical layer authentication should take the place by replacing heavy cryptographic algorithms in the ITS since 5G-AKA protocol is proven to be efficient than the latter one. IBC is needed to be adapted for the V2X communications and then, it will be wise to remove the certificate infrastructure of the ITS model. In the end, the future prospects and directions have been discussed pertinent to this research field. The existence of V2X communications came a long ago before the initiation of 5G. In that time, the security mechanisms as well as the protocol stack had been made for the standardization with the assistance of state-of-the-art technology. Nevertheless, it cannot be denied that 5G is moving towards the business end and possessing modern standards to make lives easier, comfortable, and secure for the citizens of the world. Since 5G possesses technological advancements, it is believed by many researchers that 5G will have a huge grasp over the V2X communications. However, it is needless to say that the security of 5G is needed to be analysed thoroughly and it is necessary to find efficient way to have integration with the existing ITS model.

# APPENDIX I

Cellular communication technology has already experienced numerous researches in order to provide secure, reliable and faster connection for the future generation. Thousands of proposals germane to technology and architecture have been considered by researchers in order to address the associated problems that may arise when the proposals are being executed. In addition to that, frameworks related to protect the privacy in 5G network have been proposed that concentrates on the data encryption, data obfuscation, access the control and data anonymity.

Protecting and securing the communication networks have been regarded as one of the most difficult tasks due to the difficulties in the network. In addition, the perimeter based solutions as well as the proprietary management makes it even difficult (Kamuru & Nijim, 2014). In addition, the architecture of the internet is responsible for dealing with the problems that are originated in the infrastructure (Barzoi & Luca, 2013). The revolutionary change has come up with the wireless network system which is IP-based in nature. That being said, as the time passes by, the challenges of internet-based securities have already been transferred to the wireless network system.

In the following part, the discussion will be based on the current approaches of D2D communication in case for protecting the privacy since these are very much germane to the cellular network system of 5G.

# APPENDIX II

A proposal on a particular conditional scheme called ‘privacy-preserving’ has been introduced for the vehicular network which is 5G enabled by default. It is supposed to provide the performance in real-time in addition to the identification of threats to the privacy (Azees, 2017). On the other hand, another proposal came up with the introduction of a clustering based security which would be adaptive and also, a scheme for protecting privacy for the 5G VANET (Eiza, 2017). In order to achieve data privacy in the D2D communication, relationship based scheme has been proposed by another sets of researchers (Wo et al., 2018). The devices that are already authenticated join in the data anonymity and the communication with the assistance of device nodes, participate in the operation anonymously. However, it is regarded that these particular mechanism are narrowly concentrated on the protection and is vulnerable to any devices that are not known to the mechanisms (Fan, 2018). Hence, it is evident that this particular privacy protection poses a dangerous threat to the privacy protection since the compromised device will be responsible for

sharing sensitive information with the device identities. Remote locking signals have a way of capturing as well as replicating the accessibility to a particular vehicle which is fairly accepted and acknowledged in all of the primitive systems. Moreover, it is also responsible for switching off the alarm system that allows the thieves to have ample time and opportunity to grab the vehicle and flee from the spot. The manufacturers all around the world put money in executing the systems to be top notch and unable to break the privacy protection. The usage of a cryptographic key is widely used. On the other hand, the vulnerabilities are still in the large which allow the competition to possess the access of the vehicles. Hence, the vehicles get compromised without a notice and therefore the proposal given by VANET in order to security purposes, do not meet the expectation (Eiza, 2017). There is a report published by news The Guardian which entails that the Range Rovers which possess keyless locking navigation are targeted by the thieves due to the vulnerability it possesses. On top of that, the necessity of new keys is needed to be programmed in a way that can present a significant opportunity to the thieves to take the vehicle away from the real owners. With respect to Audi RS4 vehicles, the thieves have also been able to exploit a way to drive the vehicles away by adding a new key to the system after the thieves can achieve physical access of the vehicles. Though this can be regarded as a pre-planned attack on the vehicles, the company, Audi, has refused to acknowledge any claim from the owners or the insurance companies. Some important and tricky techniques have been derived by the researchers of the University of Birmingham. They have developed keyless entries so that the encryption mechanisms can be cracked. But, the research findings were not published in the beginning since if the findings were leaked, the number of car thieves would increase and the crime rate in UK would go up (Verdult, D. Garcia and Ege, 2015).

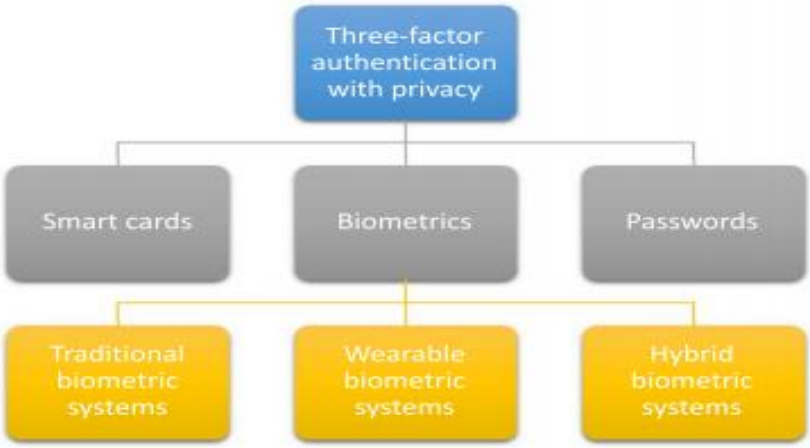
# APPENDIX II

**Three-factor authentication with privacy**

The classification of the three-factor authentication with privacy can be folded into three folds such as:

1. Protocol based on smart cards
2. Protocol based on biometrics
3. Protocol based on passwords

The following figure can portray the classification in brief with visualization:




The real question would arise on the possibility or feasibility to use the aforementioned three factors altogether. In terms of authentication protocol, the smart card can depict what the user holds, the passwords can portray what the user knows, and the biometrics can represent what the user truly is (Fan & Lin, 2009). To be exact, the author intends to propose a scheme which would be a three-factor authentication scheme so that biometric privacy can be stronger than before. Upon the authentication and login phases, the server can only accept the user if he/she can pass the authentication phases successfully (Fan & Lin, 2009). This scheme can prove to be efficient enough in case for the low computation method for the smart cards (Lin & Lai, 2004).

Hence, the biometric systems can be folded into three folds (Blasco et al., 2016), which are;

1. Traditional Biometric Systems (e.g., using Windows (Rathgeb & Uhl, 2011));
2. Wearable Biometric Systems (e.g., using smartphone (Camara et al., 2015a))
3. Hybrid Biometric Systems (e.g., in telecare services (Camara et al., 2015b))

With respect to the security concern of the biometric based identification system, it is a must for the user that he/she is unable to know anything that is on the database. That is why the usage of fingerprint is mandatory to provide higher sets of reliability (Barni et al., 2010). This identification protocol can prove to be very efficient compared to the other schemes with respect to the usage of the bandwidth (Erkin et al., 2009; Sadeghi et al., 2010). In order to render the protection of identity and to strengthen authentication system, it is important to understand the protocol of password based authentication and the service it can possibly render in the long run. Another study found that a cryptanalysis has been done on the protocol of Hsiang and Shih so that a more secure identity based authentication protocol can be found (Sood et al., 2011). In addition to that, this protocol is fairly efficient in terms of the complexity in computation compared to the multi-server authentication protocols (Hsiang and Shih, 2009; Liao and Wang, 2009). Another cryptanalysis

has been done on the proposition of Hsiang et al. where it was found that the scheme was vulnerable to huge attack which is not easily counter-attacked such as server-spoofing attack (Lee et al., 2011). Moreover, the scheme is considered as an efficient one since it is beneficial in terms of the cost of communication for the verification as well as login stages. Based on the review of the Chen et al. (2013), some authors came up with a proposal on the hierarchical identity based access authentication protocol which they have named like HA-HIBS-VN (Liu & Liang, 2013). It can be applied to the 5G cellular network. HA-HIBS-VN protocol has the capacity to provide the essence of the non-forged signature and the private key privacy (Liu & Liang, 2013). The handover delays are the thing that set this protocol efficient apart from other protocols with the combination of the identity based signature, Peer Group Tree (PGT), and Mobile Vector Network Protocol (MVNP) (Dang et al., 2010). The historical studies in that arena such as studies on the password based authentication protocol fell short to provide necessary solutions to shed some light on the attacks. Therefore, Wang et al. (2014) went on reviewing the two-factor authentication system which had been proposed by Li et al. (2013). However, in this scheme, it was discovered that it was vulnerable to the password anticipation attacks on the offline. But, the research done by Wang et al. (2014) revealed this his scheme could counter attack the password anticipation attacks and if the smart card had been lost, it would work nevertheless. That being said, the scheme is highly beneficial for the cost of computation in favour of the user's perspective. In order to get rid of the weaknesses possessed by (Das, 2011), (Li et al., 2013a, 2013b), the recommendation would be to undertake three-factor remote user authentication along with the scheme on the key agreement by utilizing biometrics. However, this particular approach does not actually go hand-in-hand with the D2D communication for the 5G cellular network since this depends upon a unique key provided by the Certificate Authority (CA). In accordance with Rajputh et al. (2017), the proposal of cloud based conditional privacy preserving mechanism is taken care of the CA. In addition, the assignment is given to the sets of devices (Rajputh et al., 2017). On the contrary, this mechanism has less utility for D2D communication as well as for 5G cellular network. A sophisticated smart card based password authentication system has been proposed which can guarantee the secrecy as well as can achieve the mutual authentication proposition (Wang et al., 2014; Chen et al., 2014). This sophisticated protocol has been discovered on the basis of two reviews from Xu et al. (2009) and Sood et al. (2010) schemes. Moreover, this particular scheme has the capacity to be efficient with respect to the computation cost on the server side which can be compared to the other schemes such as Song et al. (2010), Sood et al. (2010), and Xu et al. (2009). Hence, if in any circumstances the memory device which carries the authentication is revealed, the scheme will be more prone towards suffering the offline attacks on password anticipation (Chen et al., 2014). Three

characteristics have been discovered with a view to reviewing the schemes provided by Sood et al. (2011) and Wen and Li (2012) since these will be important for creating smart card based password authentication system sustainable. Also, it will be possible to apply in the cellular 5G network (Ma et al., 2014). The shortcomings that Chang et al. has in the scheme (Chang et al., 2013), this can be solved by adapting the assistance for the session key management system (Kumari et al., 2014a). This scheme by Kumari et al. (2014a), the user can be able to stay under the radar; means, the user will not be traceable and he/she can be anonymous. In order to overcome with the weaknesses of Kumari et al. (2014a), another proposal has been proposed stating the augmented remote authentication scheme that also serves the user with anonymity as well as privacy (Chaudhry et al., 2015).

# APPENDIX III

**pseudonym algorithm**

The pseudonym algorithm is regarded as the base of location privacy preservation framework with respect to the vehicular network for 5G (Liao, 2018). Anonymous as well as pseudonyms, both have already been utilized for the concern of privacy maintenance in numerous applications. Vehicular networks which are ad hoc can be an example in this instance (Förster, et al., 2018) . The usage of the pseudonyms and anonymous is used so that the identification of storage units cannot be known; thus, can be hidden. Hence, the threats to privacy are still concern in that arena. For example, let's assume that handful amount of power is injected by some unites for quite a period of time. The utility will able to forecast that the storage units have no redundant power which will increase the demand of the power. The forecast may be utilized in case for manipulating the purchase price so that financial gain can be achieved. The usage of data aggregation technique is better since it is able to classify the units' of storage's self bids. This method of operation is efficient in terms for the privacy of location and to classify the 5G introduced vehicles aloof from tracing whereas it is quite unable to protect the identity as well as the data privacy-preservation. In addition, it is said that the algorithm has lacking in meeting instant demand and possible leakages which make the D2D vulnerable mode of communication. For example, the hacker stays in between the utility and the storage unit and intends to setup two keys where a single key is needed to be shared with the utility and other will be shared with the storage unit so that the attackers can become fool with direct supervision. In case of a successful

attack by the hackers, they have many different options to choose from such as fabricating the bids.

# APPENDIX IV

**Homomorphic Encryption**

D2D data privacy-preserving scheme has been proposed by authors with respect to the 5G cellular network which is clearly done on the basis of homomorphic encryption (Jin, 2018). The scheme has the potential to implement a secured data which can be aggregated of the cipher text in order to protect the privacy of the data. However, the scheme has a constraint with minimal power of computing and inability to provide security against threats like snooping or eavesdropping (Liao, 2018). In case for the homomorphic encryption, the bids are generally encrypted and the encryption is done by public key. It is impossible to make the decryption without having the private key. The utility will be unable to acknowledge bids of units since gateway is responsible for sending aggregated bids to utility. Also, it is impossible to make decomposition to bids which are individual in nature. The relay meters, gateway and the eavesdroppers are unable to point out the total number of storage units' bids. It can be the huge power which is pushed from community since the community is unable to know classified keys. Also, the usage of one-time key in the aggregation along with another one-time number which is random, in case for homomorphic encryption, surely can be able to strengthen the preservation of privacy since the bids are being sent by the storage units to numerous times. In addition, if that identical key is being rejected in addition based aggregation, it is possible that the hacker might be able to calculate differences among the bids. This signifies that if a single bid is exposed, simultaneously all of the bids will be exposed automatically.

# APPENDIX V

**Patel:** What should be the role of SDOs in creating and supporting the regulatory requirements in 5G networks ?

**Piers O'Hanlon:** I think SDO's are important in terms of discussion on protocols and best practice and the SDO's then need to liaise with the regulatory authorities in the relevant jurisdictions to form appropriate regulations for the industry and international usage.

**Patel:** Can standards play a major role providing security assurance ?

**Piers O'Hanlon:** SDO's Provide important forum before the meeting of stakeholders to discuss their concerns and a shared experiences and knowledge within the limitations that the company's or have and I think they provide an important guideline and recommendations in terms of security operations and security algorithms for example than crypto algorithms hashing algorithms and their usage and then insurance can be built up from adherence to these recommendations and guidelines.

Patel: How can an international and multi stake holder dialogue help address concerns about the security and the privacy for 5G ?

**Piers O'Hanlon :** OK an international multi stakeholder dialogue is important so that other organisations can discuss their common concerns and understand the threats that they are all facing but these are all changing so it's important to kind of keep the keep the dialogue open it's also important to take into consideration user input so organisations that study feedback from users in terms of their privacy and requirements from the system .

# APPENDIX VI

**Interview**

**Patel:** What are some of the main outputs of the pre-standardisation work group ?

**Hugo Tullberg :** Well if I work with freestanding station developing a roadmap for standardization to show how the different types of PPE products in Pakistan organisation and we are targeting a release during the Fall this year and as your nose standardization is important in many aspects one of them is a business enabler for others to know what what you were here to when building new products and in particular for 5G we foresee a large number new use case is the new actors in is the actor system and therefore the standardization this is really important

**Patel:** what are the main standardization in bodies in 5g ?

**Hugo Tullberg :** Now as 5g as a larger scope than the previous generation then will not only targeting evolved mobile broadband automatic machine that communication ultra-reliable and low latency

communication services the even though it's 3pp will be the main and station body there are also a large number of other relevant standards station bodies including IETF and Xen so on and so forth and it will be mentioned in the centre Station Road map

**Patel:** How is 5G ensure the contribution to the security standards aligned with your roadmap?

**Hugo Tullberg :** When it comes to security in 5G networks this is a really interesting and new ballgame and because in the previous generations it was mostly one services that were dominating and the security solutions were optimised words that service now for 5G we foresee a large number of services which means that the security requirements and Security Solutions will be very different and it will meet the diverse needs from stronger security requirements to less strong possibly for massive machine type communication and sensor network possibly I'm saying because it all depends on the use case and the biscuit now we're fortunate in the 5pp to have the 5th gen short product to work on on this and they are an active contributor to the workgroup pre standardization I hope to see a lot of a good technical outcome coming out this product the workshop today has been very interesting and we've seen a lot of good good are use cases and initial thoughts and someone and I'm looking forward to see it the more hands-on technical results.

**Pathel :** why is 5g video surveillance is important in vehicular network ?
**Hugo Tullberg:** Vision for secure resilient enviable 5G network Consortium of 16 partners across Europe work closely for 24 months with a goal to deliver strategic impact across technology standardization and business enablement, as a result, the group formed a holistic view to incorporate privacy and trust in the 5G networks and develop software to function as a basis for the 5G network security enable.

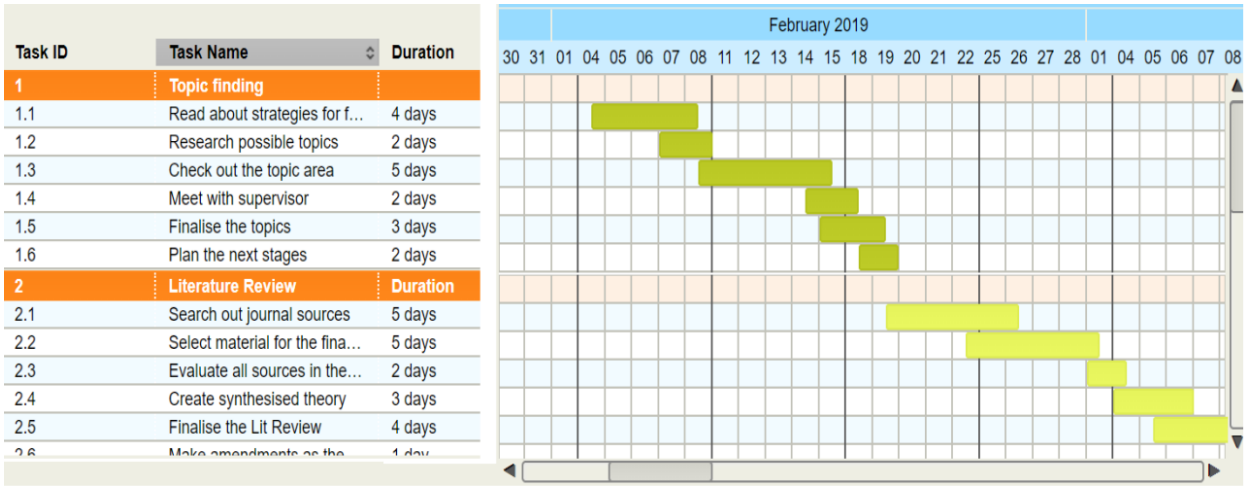
**Pathel:** What are the major security threats for the 5G networks?

**Hugo Tullberg:** 5G is going to be an important driver to implement different technologies that are currently developing like IOT, IOE and smart cities and smart farming and different other technologies. This kind of technologies help to have seamless communication between different layers and parameters and also allow the permission to have communication between all of them. Regarding to the security aspects we need a common centralization in order to get a common way to do the things, we will need a privacy features by the time we get there.

**Pathel:** What are the main recommendation to address major security threats in 5G ?

**Hugo Tullberg:** My recommendation is performed by ENISA is to face the sign of new 5G technology by the sign and to perform security in deep approach

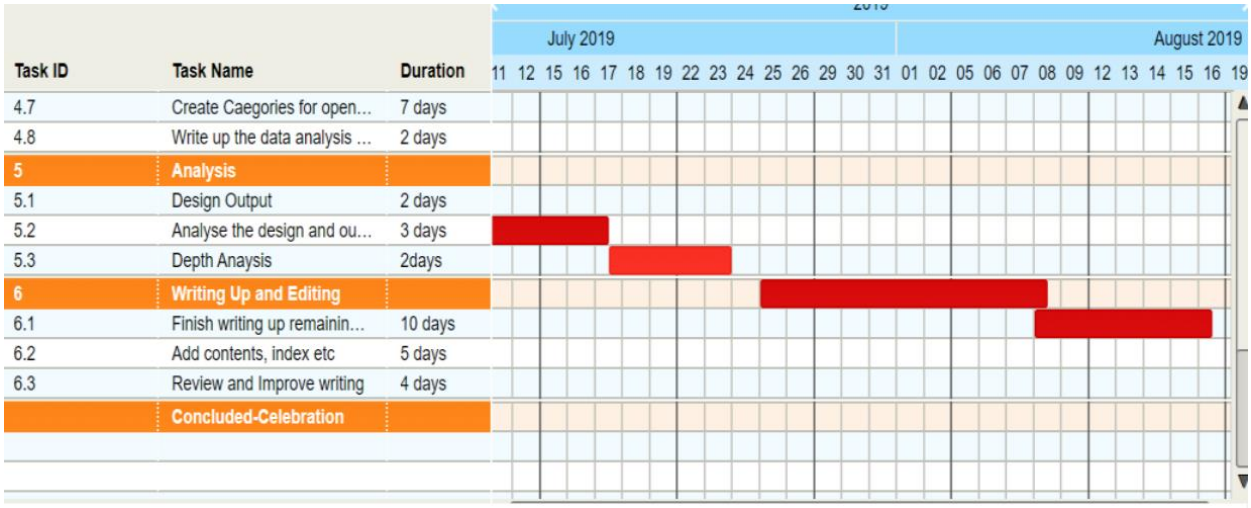
# APPENDIX VII



| Task ID | Task Name | Duration |
|---|---|---|
| 1 | Topic finding | |
| 1.1 | Read about strategies for f... | 4 days |
| 1.2 | Research possible topics | 2 days |
| 1.3 | Check out the topic area | 5 days |
| 1.4 | Meet with supervisor | 2 days |
| 1.5 | Finalise the topics | 3 days |
| 1.6 | Plan the next stages | 2 days |
| 2 | Literature Review | Duration |
| 2.1 | Search out journal sources | 5 days |
| 2.2 | Select material for the fina... | 5 days |
| 2.3 | Evaluate all sources in the... | 2 days |
| 2.4 | Create synthesised theory | 3 days |
| 2.5 | Finalise the Lit Review | 4 days |



# APPENDIX VIII

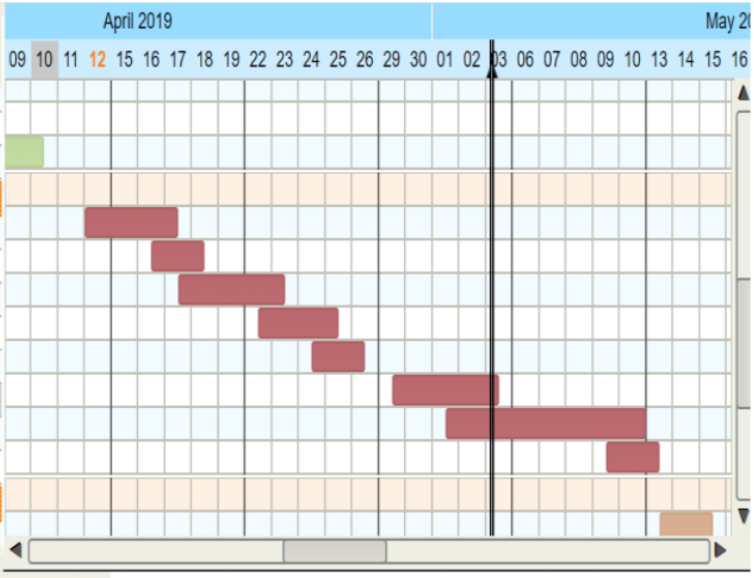


| Task ID | Task Name | Duration |
|---|---|---|
| 4.7 | Create Caegories for open... | 7 days |
| 4.8 | Write up the data analysis ... | 2 days |
| 5 | Analysis | |
| 5.1 | Design Output | 2 days |
| 5.2 | Analyse the design and ou... | 3 days |
| 5.3 | Depth Anaysis | 2days |
| 6 | Writing Up and Editing | |
| 6.1 | Finish writing up remainin... | 10 days |
| 6.2 | Add contents, index etc | 5 days |
| 6.3 | Review and Improve writing | 4 days |
| | Concluded-Celebration | |



# APPENDIX IX

| Task ID | Task Name | Duration |
|---|---|---|
| 3.3 | Create ethical statement | 3 days |
| 3.4 | Create survey or interview... | 8 days |
| 3.5 | Reflect on the effectivness... | 5 days |
| 4 | Collect Data | Duration |
| 4.1 | Short test run on methods | 3 days |
| 4.2 | Publish survey | 2 days |
| 4.3 | Carryout interviews or oth... | 4 days |
| 4.4 | Interview transcription | 3 days |
| 4.5 | Ensure data is fully collect... | 2 days |
| 4.6 | Validate data | 4 days |
| 4.7 | Create Caegories for open... | 7 days |
| 4.8 | Write up the data analysis ... | 2 days |
| 5 | Analysis | |
| 5.1 | Design Output | 2 days |



# References

Ahmed, S. A., Ariffin, S. H., & Fisal, N. (2013). Overview of Wireless Access in Vehicular Environment (WAVE) protocols and standards. Indian journal of science and technology, 6(7), 4994-5001. Retrieved 7 29, 2019, from http://indjst.org/index.php/indjst/article/viewfile/34355/27974

Aurora, R. N., Zak, R., Auerbach, S., Casey, K. R., Chowdhuri, S., Karippot, A., . . . Tracy, S. L. (2010). Best practice guide for the treatment of nightmare disorder in adults. Journal of Clinical Sleep Medicine, 6(4), 389-401. Retrieved 7 29, 2019, from https://ncbi.nlm.nih.gov/pmc/articles/pmc2919672

Barzoi, S. C., & Luca, A. C. (2013). Significance of studying the petrography and mineralogy of the geological environment of old rupestrian churches to prevent their deterioration. A case study from the South Carpathians. Journal of Cultural Heritage, 14(2), 163-168. Retrieved 7 15, 2019, from https://sciencedirect.com/science/article/pii/s1296207412000969

Bernard, H. (2011). Research Methods in Anthropology. In Research Methods in Anthropology (p. 7). AltaMira Press.

Fisher, B., & Costantino, J. P. (2006). RESPONSE: Re: Tamoxifen for the Prevention of Breast Cancer: Current Status of the National Surgical Adjuvant Breast and Bowel Project P-1 Study. Journal of the National Cancer Institute, 98(9), 643-644. Retrieved 8 22, 2019, from https://academic.oup.com/jnci/article/98/9/643/2522107

Förster, D., Löhr, H., Gratz, A., Petit, J., & Kargl, F. (2018). An Evaluation of Pseudonym Changes for Vehicular Networks in Large-Scale, Realistic Traffic Scenarios. IEEE Transactions on Intelligent

Transportation Systems, 19(10), 3400-3405. Retrieved 7 15, 2019, from http://dblp.uni-trier.de/db/journals/tits/tits19.html

Gianotti, F., Tacchini, A., Leto, G., Martinetti, E., Bruno, P., Bellassai, G., . . . Trifoglio, M. (2016). Information and Communications Technology (ICT) Infrastructure for the ASTRI SST-2M telescope prototype for the Cherenkov Telescope Array. Proceedings of SPIE, 9913. Retrieved 7 29, 2019, from https://spiedigitallibrary.org/conference-proceedings-of-spie/9913/1/information-and-communications-technology-ict-infrastructure-for-the-astri-sst/10.1117/12.2230150.full

Information Commisioner's Office. (2019). Guide to the General Data Protection Regulation (GDPR). Retrieved January 19, 2019, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Kamuru, H., & Nijim, M. (2014). Develop a solution for protecting and securing enterprise networks from malicious attacks. Proceedings of SPIE, 9120. Retrieved 7 15, 2019, from https://spiedigitallibrary.org/conference-proceedings-of-spie/9120/1/develop-a-solution-for-protecting-and-securing-enterprise-networks-from/10.1117/12.2050473.full

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. Perfusion- SAGE, 30(7), 537-542.

Northumbria University. (2018). ETHICS IN RESEARCH - POLICY STATEMENT NORTHUMBRIA UNIVERSITY. Retrieved January 16, 2019, from https://northumbria-cdn.azureedge.net/-/media/corporate-website/new-sitecore-gallery/research/documents/pdf/ethics-in-research-policy-statement-17-18.pdf?la=en&modified=20180523101744&hash=718C27A82F5BCFDC5457F7E14A091BF38A9B1351

Saunders , M., Thornhill, A., & Lewis, P. (2009). Understanding research philosophies and approaches. In Perason (Ed.), Research methods for business students (pp. 106-135). Essex: Pitman Publishing.

Visala, K. (2014). Hybrid Communication Architecture HCA. arXiv: Distributed, Parallel, and Cluster Computing. Retrieved 7 29, 2019, from https://arxiv.org/pdf/1407.4149.pdf

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.

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

Ericsson AB. 5G security – enabling a trustworthy 5G system. Ericsson whitepaper, Ericsson AB, Torshamnsgatan 21, Stockholm, Sweden, March 2018.

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 CDMAbased acoustic localization system. Proceedings of the IEEE International

Conference on Industrial Technology, 2015-June(June):3404–3411, 2015. doi: 10.1109/ICIT.2015.7125604.

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.

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.

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.

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.

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.

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.

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.

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.

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.2017.2787460.48 Bibliography

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.

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.

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

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.

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

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

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

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.

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.

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.

Ericsson AB. 5G Security-Scenarios and Solutions. Technical report, Ericsson AB, Torshamnsgatan 21, Stockholm, Sweden, June 2017. 49 Bibliography

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.

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.

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.

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.

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.

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

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

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 F06921 Sophia Antipolis Cedex - FRANCE, February 2004.

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.

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.

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. 50 Bibliography

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.

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.

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.

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.

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.

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.

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.

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.

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.

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); 51 Bibliography

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

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.

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.

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.

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.

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.

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.

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.

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.

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. 52 Bibliography

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.

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.

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.

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.

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.

Petri Luoto, Mehdi Bennis, Pekka Pirinen, Sumudu Samarakoon, Kari Horneman, and Matti Latva-Aho. Vehicle clustering for improving enhanced LTEV2X network performance. EuCNC 2017 - European Conference on Networks and Communications, pages 1–5, 2017. doi: 10.1109/EuCNC.2017.7980735.

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.

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.

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.

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 Qualcomm. Designing 5G NR. Technical Report April, Qualcomm, 2018.

Gandeva Bayu Satrya and Soo Young Shin. Security Enhancement to Successive Interference Cancellation Algorithm for Non-Orthogonal Multiple Access 53 Bibliography

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

Adi Shamir. IDENTITY-BASED CRYPTOSYSTEMS AND SIGNATURE SCHEMES. Advances in Cryptology - CRYPT0 ’84, LNCS 196, pages 47–53, 1984.

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 networks : A Review. China Communications, pages 1–14, 2017.

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.

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.

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.

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.

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.

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.

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/ietnet.2017.0138. 54 Bibliography

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.

Datong Xu, Pinyi Ren, Qinghe Du, Li Sun, and Yichen Wang. Design forNOMA : Combat Eavesdropping and Improve Spectral Efficiency in the TwoUser Relay Network. GLOBECOM 2017 - 2017 IEEE Global Communications Conference, (61461136001), 2017.

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.

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.

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.

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 OptoElectronics and Communications Conference (OECC) and Photonics Global Conference (PGC), pages 1–4, 2017. doi: 10.1109/OECC.2017.8114757.

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.

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.

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.