Sami Takanen

5G IMPLEMENTATION PLAN
Frequency scanning

Master's thesis

Cybersecurity
CSKT19SY

2021

XAMK

South-Eastern Finland
University of Applied Sciences

XAMK
South-Eastern Finland
University of Applied Sciences

Author (authors)	**Degree title**	**Time**
Sami Takanen	Master of Engineering	April 2021

Thesis title

5G Implementation plan
Frequency scanning

60 pages

Commissioned by

Steveco Ltd.

Supervisor

Vesa Kankare

Abstract

The objective of the thesis was to offer research insights concerning the frequency scanning within the harbour area for the port of Kotka, Mussalo. The focus was on reporting and addressing the issues in different frequency bands operating in the harbour. The structure of the thesis begins with a literature review of the 5G technology, where all the essential facts are explained. The second part recognises the cybersecurity issues concerning 5G networking, followed by the major contribution of this thesis project i.e., assessment of the 5G implementation plan; frequency scanning in the port of Kotka, Mussalo.

The research methodology employed quantitative assessments to conduct multiple frequency measurements within the harbour to find out how the harbour area is affected by different frequency bands and exploration of the possible causes for unexpected interference incidents that happened within the port area.

The frequency scanning verified that the port of Kotka, Mussalo has optimal conditions to build the 5G network within the spring of 2021, given that the different networks operating within and affecting the harbour area are unimpacted by any unwanted actions. However, the interference incidents (i.e., the connection losses) reported previously within the harbour were not faced during the study. Also, since during the scanning period, enough ship traffic was not encountered, the only likely cause of interference incidents identified is the ship landing and leaving because of the radar systems used.

Although due to lack of interference incidents the third goal was not achieved, the thesis successfully achieved the first and second goal by introducing the basic elements and operations of 5G networking and finding out the frequency bands operating in the harbour area.

Keywords

5G, cybersecurity, frequency scanning, monitoring

CONTENTS

1 INTRODUCTION

Harbour areas generally involve various modes of traffic, such as ship, train, and truck traffic. This creates a very crucial point in maintaining security and control within harbours and to sustain a safe and reliable environment. And thus, the network security within harbours has been regarded as one of the most critical issues. Thereby, communications inside the harbour areas have mainly relied on wired connections. Further, camera surveillance is implemented to enhance the supervision within the harbours. It offers information for the operators in the control rooms.

During the years, mobile networking solutions have been increasingly deployed to serve the crew working in ship cranes and straddle carriers. Firstly, the reason why mobile networking solutions have been implemented is the fact that wireless networking solution (WLAN) has not been as reliable as the mobile telecommunications. Secondly, in wireless solutions, it has been noticed that to build a network, which is sufficient to maintain the needs and requirements, the need for WLAN repeaters makes the environment too expensive and heavy to maintain.

When the 4G standard was introduced in 2008, it promised to revolutionize the whole networking. Because of the high-speed connections, the 4G indeed took the mobile networking to a different level compared to the earlier 3G standard. The harbour areas were deeply interested in 4G technology because of greater speeds with lower latency. Different test networks were deployed to find out how the camera data can be transferred to the control rooms and monitored on a real-time basis. Some solutions found out to be effective, but the major drawback was the expenses (WIlsonAmplifiers 2021).

In 2018 when 5G was introduced there were high expectations for the world to become more interconnected where people are expected to connect different smart devices to their home networks. The concept of IoT (Internet of Things) also surged as one key concept in the 5G development. Similarly, harbour areas also showed enthusiasm after multiple unsuccessful attempts with different solutions, such as WLAN and 4G technologies. The 4G failed to meet the requirements for upload speeds of the connections, and WLAN was found exorbitant to cover the necessary points in the harbour areas. Specifically, within the Mussalo harbour area, one pre-5G network has already been deployed for networking test needs. It is being used to assess how the greater speeds of networking meet the requirements of the camera data transition, from container cranes to the control rooms.

This 5G technology research is carried out to investigate, how the newest generation of technology can gain more performance in the mobile connections within harbour areas with fewer latency times.

2 RESEARCH

In the spring of 2020, discussions were held to find out possible research projects for the master’s thesis work. One project identified was to facilitate the future research needs in the upcoming 5G networking implementation in the port of Kotka, Mussalo in the spring of 2021. The port of Mussalo is a leading container port in Finland specialised in container operations. It provides a full range of container terminal services with a handling capacity of about one million TEUs. It also serves as a container transit port in addition to export traffic (Steveco Ltd. no date). This project was commissioned by Steveco Oy in collaboration with the XAMK 5G FINLOG project.

2.1 Research problem

In the harbour areas, camera surveillance has an important role in supervising the whole harbour vicinity and in maintaining high levels of security in the area. During the years, Steveco Ltd. has implemented different mobile or wireless networking solutions to maintain the high level of camera surveillance on their property. All the solutions delivered so far have been unsatisfactory because of the costs and upload speeds of connections. Therefore, in 2020, Steveco Ltd. started to plan the deployment of the latest mobile networking technology, i.e., 5G, due to its promising specifications particularly to the harbours, such as the camera surveillance, the capacity to transfer the camera data from container cranes to the control rooms and the provision for real-time monitoring. However, a major problem that requires attention is the inadequate upload speeds of connections in transferring the camera data with fewer latency times. The second problem is the loss of connections when certain ships are landing and leaving the harbour. There is a need to address the cause of possible interferences and to explore how to maintain more stable connections. Thirdly, it is also vital to find out the possible cyber issues 5G networking can encounter while operating. The harbour areas are crucial business points which need to take the risk management process into account when applying actions for unexpected incidents.

2.2 Research objectives

The research was carried out to fulfil the needs of the harbour where Steveco Ltd. is managing the harbour traffic. The challenges encountered within camera data transmission from the container cranes and camera surveillance, altogether, made Steveco Ltd. start a project of planning the implementation of 5G networking within the harbour area, especially within container field. In the spring of 2020, the project started in collaboration with XAMK 5G FINLOG project team. XAMK 5G FINLOG project saw an opportunity to conduct research in understanding what kind of environment it is for implementing a 5G network and to enhance the performance of camera surveillance.

Hence, the objectives in the thesis are,

- to find out the frequency bands used in the harbour area,
- to analyse all possible origins for interference incidents, and
- to research 5G networking technology and its cybersecurity aspects.

2.3 Research questions

The research process for this thesis work can be divided into three sections, theory, practical, and future insights. The theory part consists of the 5G networking and the specific cyberthreats associated to this newest mobile networking technology. The practical part, which is the main component of this thesis, consists of the frequency measurements within the harbour area, finding out the frequency bands being used that have an impact on the harbour operations and the analysis of unexpected connection losses encountered during the time certain ships land /leave and the possible causes of these incidents. The measurements also provide information which can be used to monitor the network traffic flow in the harbour area in the future, while the future part constitutes the recommendations for future networking planning and implementations. As a result of this analysis, Steveco Ltd. will be aware of the network traffic in the harbour area and may be better equipped to launch adequate planning and implementation of network monitoring solutions to improve the maintenance of the property in the future.

The main research questions are as follows:

1. What kind of frequency bands can be scanned within the port of Kotka, Mussalo?
2. Why is the harbour area facing connection losses?
3. How is cybersecurity considered in 5G?

2.4 **Methods**

The empirical research project was informed and executed following the literature review where all the essential material pertaining to 5G networking was analysed to gain a holistic understanding of mobile networking technology, while the quantitative assessment was chosen when making the frequency measurements in collaboration with the XAMK 5G FINLOG project leaders.

2.5 **Frequency scan**

The practical part of this thesis project was executing the frequency measurements within the harbour area. The first set of measurements were made by Rohde & Schwarz PR200 Portable Monitoring Receiver, which is used for monitoring spectrum and interferences. The specific features applied in this project were frequency sweep, polychrome scan, and level mapping. The frequency sweep and polychrome scan identified the frequency spectrum at different frequency bands. The level mapping feature was used to create a map of the container field with the strength of the frequency spectrum yielded (© Rohde & Schwarz; R&S®PR200 Portable Monitoring Receiver 2020).

The second measurements were carried out to meet the requirement of XAMK 5G FINLOG project, as well as to get additional information with different testing tools. In the second measurements, the R&S Scanner (R&S®TSME6) and R&S Drive Test Software (R&S®ROMES4) were used. The features used in the measurements were “Automatic Channel Detection” and “Spectrum Scan” and “Coverage Analysis”.

3 THE FIFTH GENERATION OF MOBILE NETWORKING (5G)

The fifth-generation technology standard of cellular networks was introduced in 2018. The main improvements in 5G technology are the greater speed and the lower latency times. This has revolutionized the whole networking schema and has led to so many devices nowadays being connected to the Internet. In the early days, only wired connections carried the speeds the devices and locations needed, however, these days the high-speed connections are supported by mobile networking technologies. Wired connections are no longer invested as the only option to the locations with a challenging environment because of the revolution that happened in mobile networking technology development from 3G to 5G (Tripware Inc. 2020).

Data rates of over 2 Gbit/s and the ability to revolutionize the network infrastructure are the main descriptions for the 5G networks. In the design, the planning is more accurate with 5G because of the millimeter-wave spectrum. The millimeter-wave spectrum is more sensitive to different kinds of obstacles and materials. And thus, trees and even weather have a significant impact on how the 5G spectrum works. This is called "ground clutter", which is one of the biggest challenges in network planning (TEOCO no date). The ability to carry huge amounts of bandwidth has made it a remarkable element in the 5G standard development (TEOCO no date). However, the sensitivity of the 5G millimeter-wave spectrum is a challenge to the next generation of wireless communication technology.

Planning a 5G network in the existing infrastructure is not just implementing the system with its new features, but also analysing the requirements for the millimeter-wave spectrum to deliver the best features of 5G networking. All the information of the environment needs to be gathered for the 5G planning process to form a 360-degree view of the environment and design an optimized and cost-efficient network (TEOCO no date). The licensed frequency bands in 5G networking are from 450MHz to 6GHz. The millimeter-wave frequencies span to 52,600 GHz. Besides, there are also unlicensed spectrums for use. This means that 5G has all the previously introduced spectrums from the older cellular networking standards, but also includes totally new ones. The additional spectrums are available for 5G is because 4G provided 5-20 MHz of bandwidth per channel, whereas 5G can provide 5-100 MHz of bandwidth per channel (Arrow 2019).

5G networking involves the crucial enhancement of the performance, but at the same time, the cybersecurity side is getting jeopardised because of the many new features implemented. Professionals are considerate towards the many vulnerabilities in 5G networking due to its susceptibility to cyberattacks. Further, when the centralized network with hardware-based switching goes to distributed, software-defined digital routing, the software is taking care of the network and cyber hygiene cannot be practiced. (Tripware Inc. 2020). Also, the extended bandwidth used in 5G opens multiple potential chances for the attackers to attack. Further, the capability to interconnect more devices (IoT) to the networks also invites vulnerable points in the network, however, the weakest point is the security side of devices (Tripware Inc. 2020).

3.1 **Millimeter-wave spectrum (mmWave)**

In 5G mobile networking technology, the millimeter-wave spectrum was the major improvement enabling the usage of higher frequency bands from 24 GHz to 100 GHz. The implementation has been in progress for a long time because of the issues with higher path loss, reduced scattering, and increased challenge with non-line-of-sight paths. These challenges are met by developing solutions like massive MIMO, beamforming, and the use of small-cell or ultra-cell densification (Al-Hazemi, Al-Mekhlafi & Shaddad 2019). Millimeter-wave spectrum brings numerous benefits to modern-day mobile communications with larger bandwidth and smaller antenna elements, which make it possible to deliver gigabit-speed of connections in wireless services. Now in the development of millimeter-wave spectrum technologies, the bandwidth has been restricted to 800 MHz for operator below 40 GHz and 2 GHz above 50 GHz frequencies.

In the millimeter-wave spectrum, the blocks being used are divided into different sections, which depict the frequencies and official band name for specific frequencies. The blocks are listed in table 1 below (Holma, Toskala and Nakamura 2020).

Table 1. The available spectrum blocks in millimeter-wave (Holma, Toskala and Nakamura 2020)

Frequency (GHz)	Band (GHz)
24.25–27.5	26
27.5–29.5	28
37–43.5	40
57–64	60 (V-band)
71–76	70 (E-band)
81–86	80 (E-band)
92–95	90 (W-band)

3.2 Massive MIMO (multiple-input multiple-output)

Massive MIMO is a technology (that has been) deployed into many wireless systems from Wi-Fi to mobile networking like 4G, and now also in 5G. In 5G technology, Multi-User-MIMO (MU-MIMO) will be used to utilise the distributed and uncorrelated spatial location of the various users (Huang et al. 2017). The MU-MIMO operates in a 5G base station by sending a CSI-RS (Channel State Information Reference Signal) to the user equipment and then computes the spatial information for each user. The information is used for computing the required information for the pre-coding matrix (W-Matrix) for the data symbols to be constructed into the signals for each of the elements of the antenna array (Huang et al. 2017).

The data streams have their weightings where the phase offsets to each stream are included to enable the waveforms to interfere at the receiver. As a result, the strength of the signal will be maximized to the user and the interference will be minimized to other users. 5G base station can communicate to multiple devices at the same time and independently when spatial information is being used. The user equipment can be operated without the knowledge of the channel or processing to attain the data streams (Huang et al. 2017). 5G MU-MIMO scales the usage of antennas by antenna arrays used in 5G base stations, which is anticipated to lead the capacity gains while using much simpler UE devices (Huang et al. 2017). A complex location, such as harbours, where different container fields can leave uncovered spots, are now reachable because of the massive MIMO implementations, including spatial diversity and spatial multiplexing (Qualcomm 2019).

3.2.1 Distributed MIMO

Distributed MIMO is introduced to improve the connection reliability and minimize inter-cell interference by increasing the signal power by using two or more cells to do the transmission to the user equipment (UE). In the same context, Coordinated Multipoint Transmission (CoMP) and Multi-Transmission Reception Point (TRP) are introduced as a synonym to dMIMO (Distributed MIMO) (Holma, Toskala and Nakamura 2020). Figure 1 demonstrates the mechanism of dMIMO. It shows how three radio units simultaneously send data to a single UE. In this process, the central unit controls the transmission with low latency connections to radio units. This leads to improvements in data rates, especially in the cell edge and in big events, where a large number of people are requesting wireless services at the same time (Holma, Toskala and Nakamura 2020).

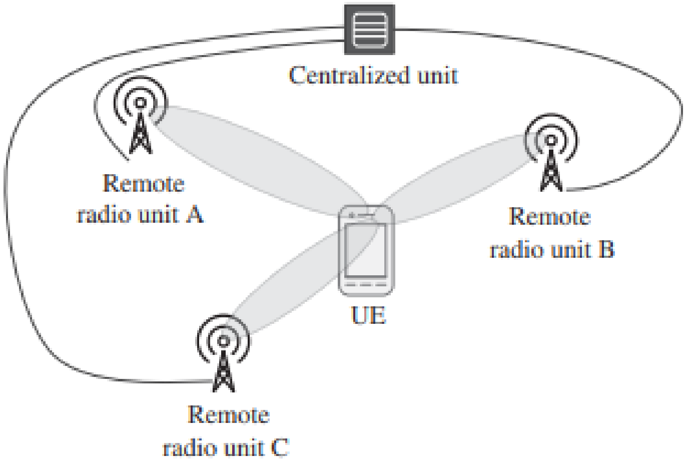


Figure 1. Distributed MIMO demonstration (Holma, Toskala & Nakamura 2020)

3.3 5G New Radio (5G NR)

5G New Radio (5G NR) was developed to provide remarkable enhancements in flexibility, scalability, and efficiency in power usage and spectrum (Huang et al. 2017), providing communications for a very high transmission band for streaming videos and low latency times for remote control, for example, vehicle communications (Electronics Notes no date). It has new elements which meet the requirements for modern-day high-speed connections. New radio spectrums are deployed for 5G NR use, which expand the frequency range from 2.5 GHz to 40 GHz and both 3.3 GHz to 3.8 GHz and 4.4 GHz to 5 GHz for immediate deployment. The spectrum of 3.3 GHz to 3.8 GHz has been released in countries, like, USA, Europe, and some Asian countries (Electronics Notes no date).

The advantages in higher frequency bands are the wider bandwidths and higher data rates, but the disadvantage is the shorter range. On the other hand, the shorter range will follow greater frequency re-use in some cases (Electronics Notes no date).

3.3.1 Design principles of 5G NR

The 5G NR wireless access methods are developed with the three technologies in mind that are enhanced mobile broadband (eMBB), massive machine-type communications (mMTC) and ultra-lean low-latency communications (URLLC) (The Ericsson Blog 2017).

While the fundamental design principles in 5G NR highlighted in Ericsson’s blog revealed are flexibility, forward compatibility, and ultra-lean. Figure 2 illustrates the design principles.

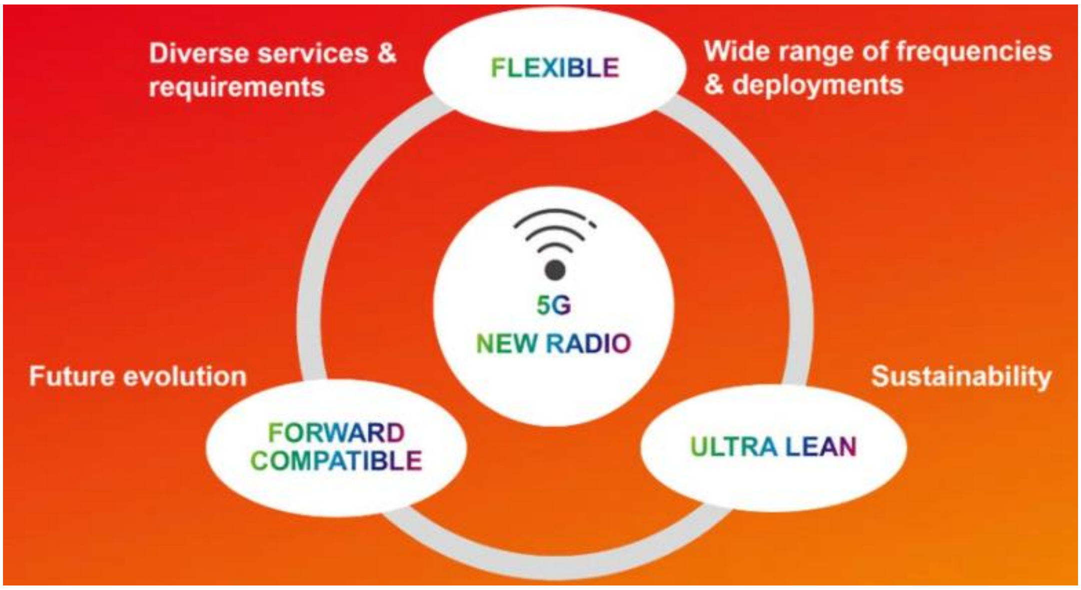


Figure 2. Ericsson's idea of three design principles of 5G NR (The Ericsson Blog 2017)

As can be seen in Figure 2, the first principle is flexibility, which is important thinking how a wide range of frequencies (sub 1 GHz to 100 GHz) are allocated to 5G technology. Also, different deployment types and diverse use cases make flexibility a crucial design principle for the 5G NR (The Ericsson Blog 2017).

The second principle is forward compatibility, which marks the independent transmissions from different data slots and beams. This is defined as self-contained transmission. The other transmission type is defined as well-confined transmission, where the transmissions are kept confined in frequency and time domain. This will allow the new types of transmissions in parallel with legacy transmissions in the future (The Ericsson Blog 2017).

5G New Radio has multiple reference signals, which are demodulation, phase tracking, sounding, and channel state reference signals. The last principle is ultra-lean design, where the idea is that networks transmit these reference signals just when necessary, which is concentrating on improving the efficiency in energy and reducing the network operational expenses (The Ericsson Blog 2017).

3.3.2 OFDMA

Orthogonal Frequency Division Multiple Access (OFDMA) is a multicarrier technology subdividing the available bandwidth into a multitude of mutual orthogonal narrowband subcarriers (ScienceDirect no date). These subcarriers can be shared between multiple users. In LTE, the OFDMA was used for the downlink and SC-FDMA for the uplink. In 5G NR, OFDMA is used in downlink but also for the uplink. The advantages and disadvantages of OFDMA are listed in table 2 below (Fitzgibbons 2019).

Table 2. The advantages and disadvantages of OFDMA (Fitzgibbons 2019)

Advantages	Disadvantages
Higher diversity and the efficient usage of frequency	The diversity of frequencies depending on how subcarriers are assigned to users
Lower interference between cells	Always on standby mode to send a transmission. → The need of extra power

Enhanced coverage over networks	Higher sensitivity compared to other channel types

The groups of subcarriers are called resource blocks and these resource blocks are referred to as sub-channelization. In sub-channelization subchannels are defined, which can be shared with mobile stations depending on the conditions on the channel. The advantage of sub-channelization is that the OFDMA system can share more transmit power to devices with lower SNR and reduce the power to devices with higher SNR within the same time slot (Ahmadi 2019).

3.3.3 Radio Protocols

The radio protocols in 5G consist of a user plane (UP) and a control plane (UP). The user plane is in the OSI model of networking between IP and physical layer and it is referred to as the Data Link Layer. In 5G New Radio (5G NR), the user plane can be divided into four sublayers, which can be seen in Figure 3 (Holma, Toskala, and Nakamura 2020).

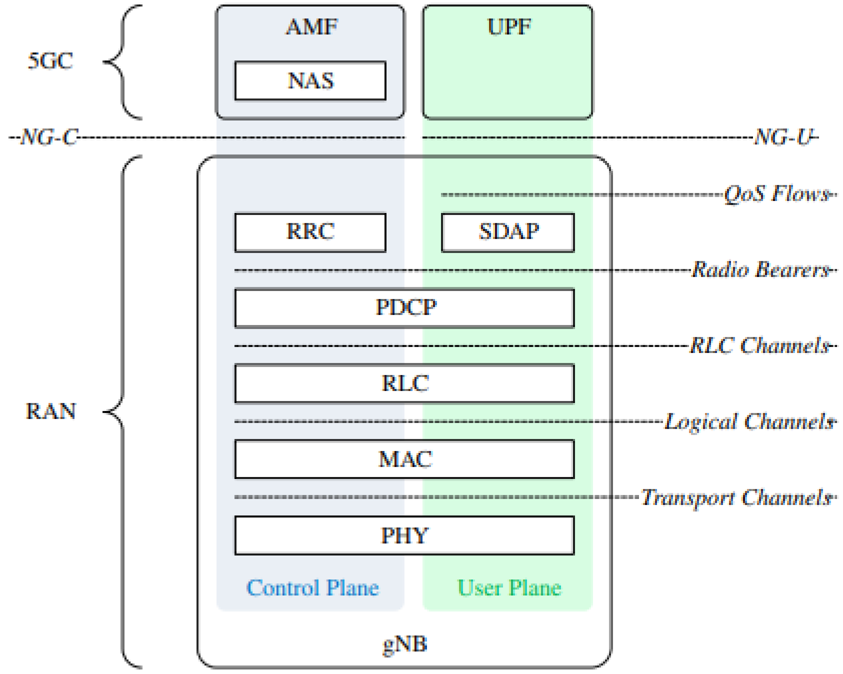


Figure 3. Radio Protocols (Holma, Toskala and Nakamura 2020)

As can be seen in Figure 3, Service Data Adaptation Protocol (SDAP) offers the quality of service (QoS) to the UPF in 5GC. Packet Data Convergence Protocol (PDCP) offers radio bearers to SDAP. Radio Link Control (RLC) provides RLC channels to PDCP. Medium Access Control (MAC) offering logical channels to RLC. SDAP is only used with standalone 5G architecture (Holma, Toskala, and Nakamura 2020).

The control plane consists of the Radio Resource Control (RRC), which is below the Non-Access Stratum (NAS) protocol of the AMF in 5GC. The Access and Mobility Management Function (AMF) is on the core side and processes on the control plane. AMF provides access authentication, access authorization, NAS ciphering, and integrity protection. Other key functionalities include the transport session management (SM) messages between UE and the Session Management Function (SMF) and supporting location services between UE and the Location Management Function (LMF) (Holma, Toskala and Nakamura 2020).

3.3.4 Beamforming

Beamforming has become a major technology in recent years, and it offers remarkable advantages in 5G. The beam from the base station towards the mobile is enabled and can be directed whilst cutting the interference to other end devices (Electronics Notes no date).

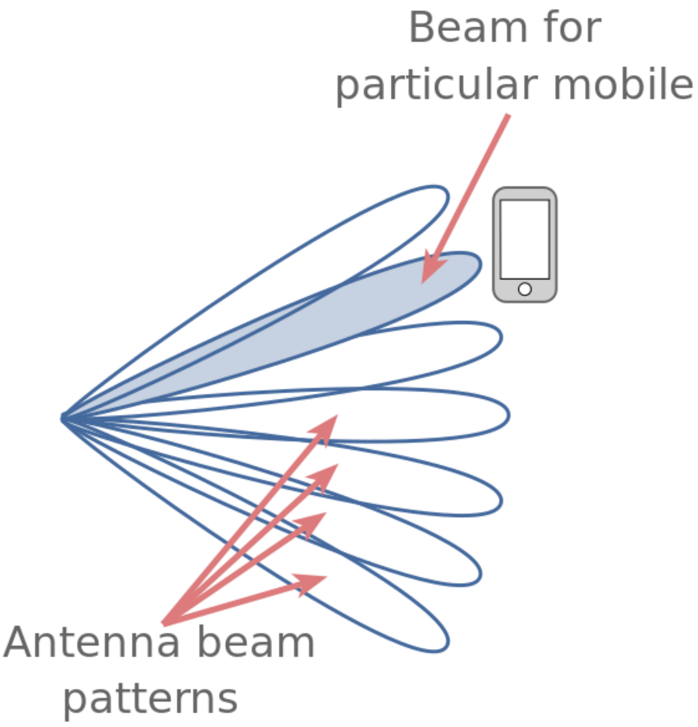


Figure 4. Beamforming used in 5G (Electronics Notes no date)

In 5G technology, beamforming is fully supported. The higher frequencies allow the usage of smaller antennas, and programmable high directivity levels are possible to be implemented. This enables directing the power to the mobile and providing receiver gain in this direction (Holma, Toskala, and Nakamura 2020). The frequency bands below 2.5 GHz the UE can support 4 beams with the subcarrier spacing 15 kHz or 30 kHz. The limit of 8 beams are supported between 2.5 GHz and 6 GHz. The mmWave frequencies with 120 kHz and 240 kHz subcarrier spacing 64 beams are supported (Holma, Toskala, and Nakamura 2020).

3.4 Dual connectivity with LTE

In 5G mobile networking technology, the radio solution is made to provide a seamless experience by enabling dual connectivity with LTE networks. 5G user equipment can have simultaneous connections to a 5G radio network and LTE radio network. The two architectures can be used to provide dual connectivity between 5G and LTE radio networks. The first option is called Option 3x which works with non-standalone (NSA) architecture. In Option 3x 5G base stations (gNodeB) and LTE, base stations (eNodeB) are connected to the Evolved Packet Core (EPC). In this architecture, the control plane goes via LTE. Option 2 is working with standalone (SA) architecture. In SA architecture, 5G core network (5G-CN) is used, which will provide lower latency because no communication is needed between 5G and LTE protocols (Holma, Toskala, and Nakamura 2020).

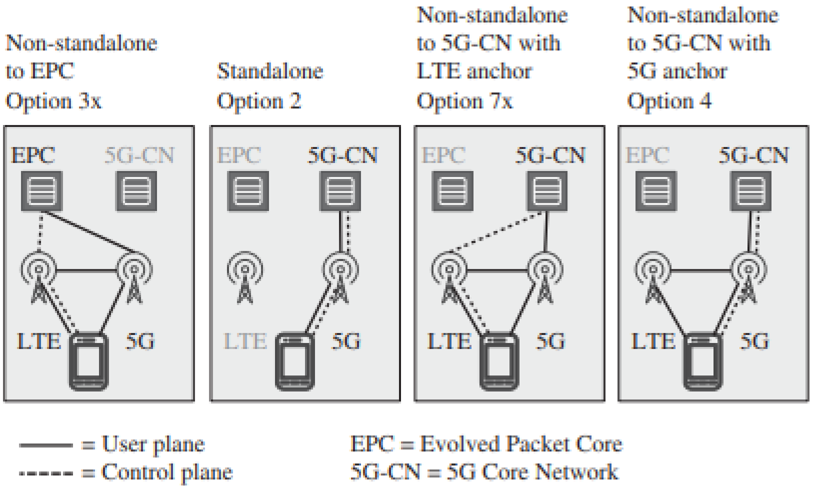


Figure 5. Dual connectivity architecture options (Holma, Toskala and Nakamura 2020)

NSA architecture will be later available with both 5G and LTE radio networks, where they can be connected to the 5G core network (5G-CN). In this additional Option 7x and Option 4, the control plane traffic can also be directed via 5G or LTE. These different options are illustrated in Figure 5 above (Holma, Toskala, and Nakamura 2020).

3.5 Cybersecurity in 5G

5G technology brings many advantages by allowing more devices to be connected to networks and ensures greater speeds and bandwidth. The scalability and flexibility in 5G technology have also been taken into the next level when network control has been transferred from hardware to software defined networking (SDN) and network function virtualization (NFV) software (Ahmad et al. 2017). The threats in 5G networking are high-number of end-users and IoT, the security of radio interface, user plane integrity, service-driven constraints on the security architecture leading to the optional use of security measures, and roaming security issues, DoS attacks on infrastructure and end-users, and signalling storms (Ahmad et al. 2017). On the other hand, NFV has security challenges, for example, confidentiality, integrity, authenticity, and nonrepudiation. Before 5G networks, mobile networks had dedicated communication channels (GTP / IPsec tunnels). SDN-based 5G networks do not have them but having common SDN interfaces can increase the possibility for attacks using this openness (Ahmad et al. 2017).

Lack of security implementations in IoT devices can lead to breaches and attacks. Larger bandwidth in connections challenges the security monitoring when traffic loads are expanded crucially. New implementations for monitoring the traffic need to be created and deployed to networks. Security solutions can be implemented but, in the end, it is the end-user, who needs to understand how to use the new technology right and safe (Kapersky 2020). Figure 6 shows how 5G operates and how different threats exist in normal communication channels. The challenges in 5G are presented in Figure 6 highlighted by Next Generation Mobile Networks (NGMN).

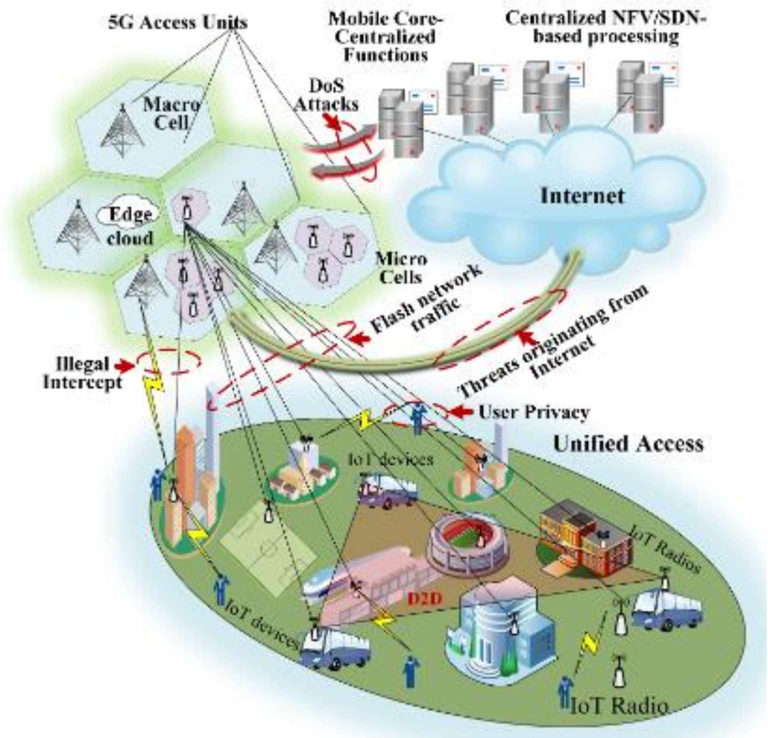


Figure 6. 5G Network and threats (Ahmad et al. 2017)

Flash network traffic describes the growing amount of end-user devices and the Internet of Things (IoT). The insecure channels are used to send radio interface encryption keys, and this makes the security of radio interfaces a big security challenge. The lack of cryptographic integrity protection for the user plane creates vulnerability in the user data plane. The security compromises with roaming are caused by the out-of-date user-security parameters with roaming from one operator to another (Ahmad et al. 2017).

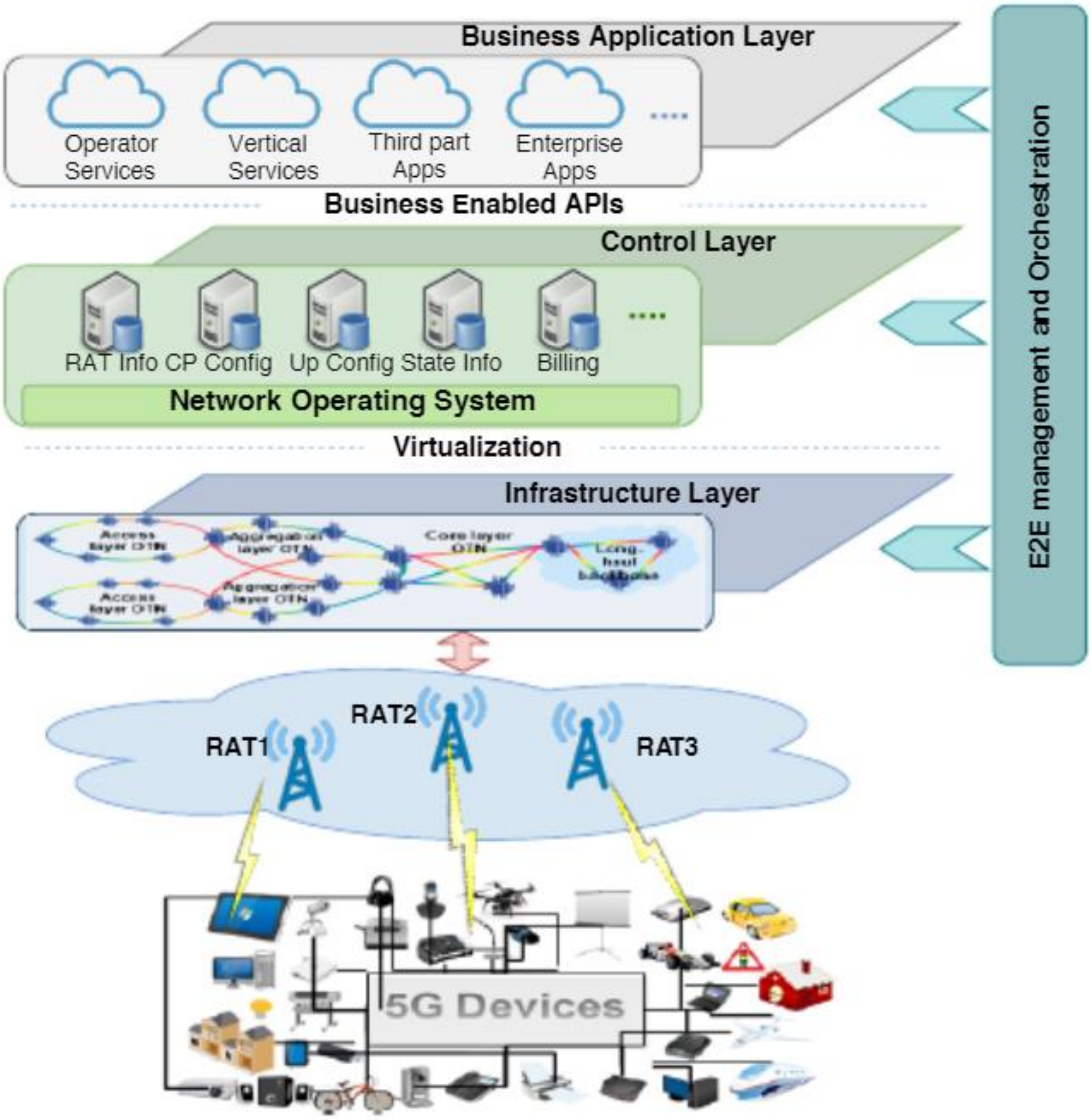


Figure 7. The Architecture of 5G in different operational layers (Khan et al. 2019)

As shown in Figure 7, the bottom layer represents all 5G devices including mobile phones and IoT devices. These 5G devices are connected to the 5G network by these Radio Access Technologies (RAT). New radio technologies are also introduced with 5G networking, for example, NOMA (Non-Orthogonal Multiple Access), massive MIMO, mmWave, and other IoT technologies (Khan et al. 2019). The infrastructure layer consists of BS (Base Stations), routers, and switches. The control layer is working in (a) collaboration with the business application layer. All the services are implemented in the business layer, but the control layer can translate the network service requests as control commands from the business layer and deliver the requests to the infrastructure layer (Khan et al. 2019).

3.5.1 Radio Access Network (RAN)

In the 5G New Radio (5G NR), the security is guaranteed via ciphering and integrity protection. The integrity protection was already introduced in LTE, where the signal radio bearers (SRB) were protected, but in 5G the protection is not limited to SRBs. The protection can be configured also for DRBs. PDCP obtains the integrity protection function including protection in the transmitter and integrity verification at the receiver, resulting in a 32-bit MAC-I at the end of PDCP PDU. The ciphering function of PDCP processes ciphering in the transmitter and deciphering at the receiver. The data portion of SDAP PDU is ciphered. The header of SDAP is left unciphered allowing the data routing in the receiver before deciphering. In Figure 8, the integrity protection and ciphering in the RAN are depicted (Holma, Toskala, and Nakamura 2020).

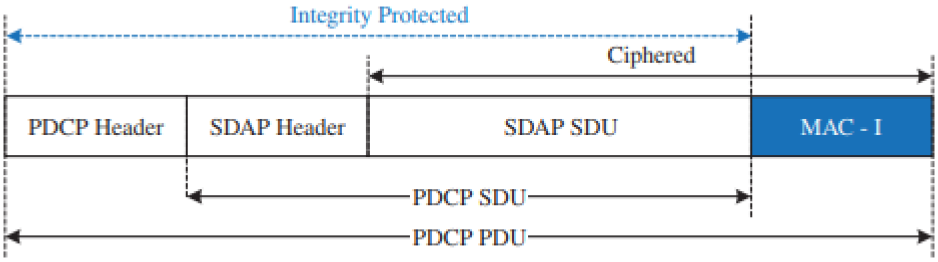
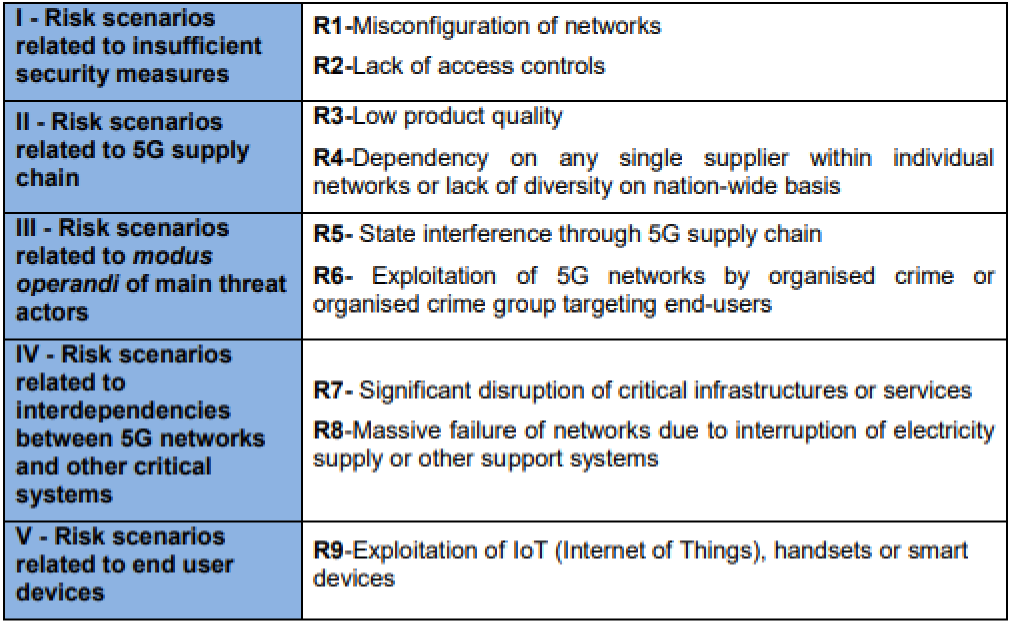


Figure 8. The integrity protection and ciphering (Holma, Toskala and Nakamura 2020)

3.5.2 EU Toolbox

EU coordinated risk assessment report (2019) identified the aim of mitigating cybersecurity threats in 5G mobile networking. The objective was to have a coordinated European based approach to 5G cybersecurity with an intention of creating the framework of security measures that ensures adequate level of cybersecurity of 5G networks across the EU among Member States (NIS Cooperations group 2020). The EU coordinated risk assessment identifies several categories of risks of strategic importance from an EU perspective illustrated by concrete risk scenarios (NIS Cooperations group 2020). The risk categories and scenarios are presented in table 3 below.

Table 3. Risk categories and scenarios (NIS Cooperations group 2020)



I - Risk scenarios related to insufficient security measures	**R1**-Misconfiguration of networks **R2**-Lack of access controls
II - Risk scenarios related to 5G supply chain	**R3**-Low product quality **R4**-Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis
III - Risk scenarios related to *modus operandi* of main threat actors	**R5**- State interference through 5G supply chain **R6**- Exploitation of 5G networks by organised crime or organised crime group targeting end-users
IV - Risk scenarios related to interdependencies between 5G networks and other critical systems	**R7**- Significant disruption of critical infrastructures or services **R8**-Massive failure of networks due to interruption of electricity supply or other support systems
V - Risk scenarios related to end user devices	**R9**-Exploitation of IoT (Internet of Things), handsets or smart devices

The EU toolbox is a recommendation for the Member States and/or the Commission, and it is included with a set of key actions. The Member States should:

- strengthen security requirements for mobile network operators, including, for example, access control mechanisms, rules on both secure operation and monitoring;
- apply relevant restrictions for suppliers considered to be high risk – including necessary exclusions to effectively mitigate risks – for key assets defined as critical and sensitive in the EU-wide coordinated risk assessment,. covering, for example, core network functions, network management, and access network function;
- avoid or limit any major dependency on a single supplier and verify the adequate balance of suppliers at a national level and avoid dependency on suppliers considered to be high risk. Require the avoidance of lock-in with a single supplier by including the greater interoperability of equipment.

(NIS Cooperations group 2020).

In July 2020 EU Member States published the report on the progress, which revealed the progress of the Member States made in certain areas, such as regulations for 5G security, the involvement of suppliers based on the risk profile and network security and resilience requirements for mobile operators (NIS Cooperations group 2020).

Some measures were also found as a lower state of implementation, for example, mitigating the risk of dependency on high-risk suppliers and designing and imposing appropriate multi-vendor strategies for individual operators at a national level. The different types of measures are identified in the EU toolbox as strategic, technical, and supporting measures as shown in Figure 9 (NIS Cooperations group 2020).

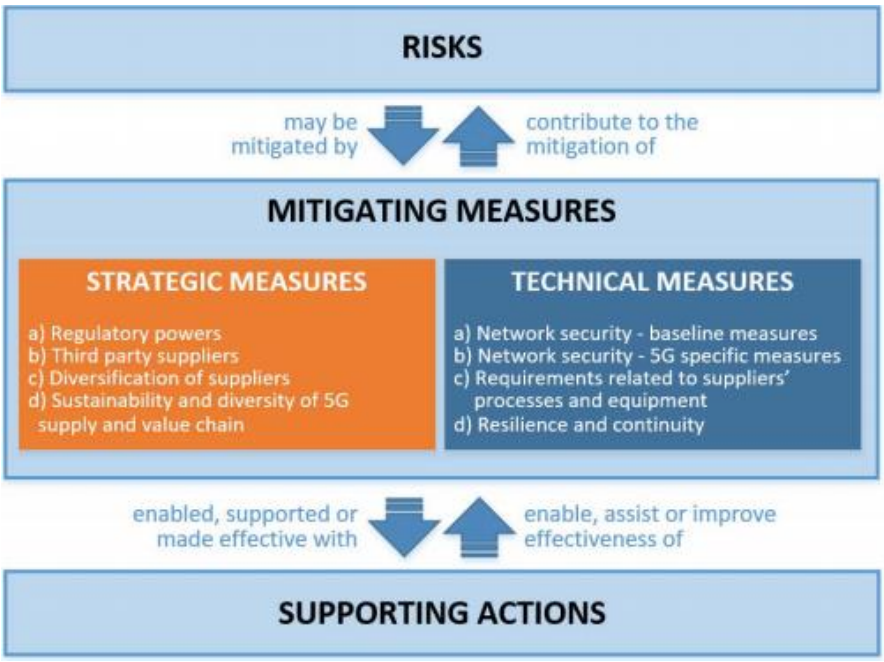
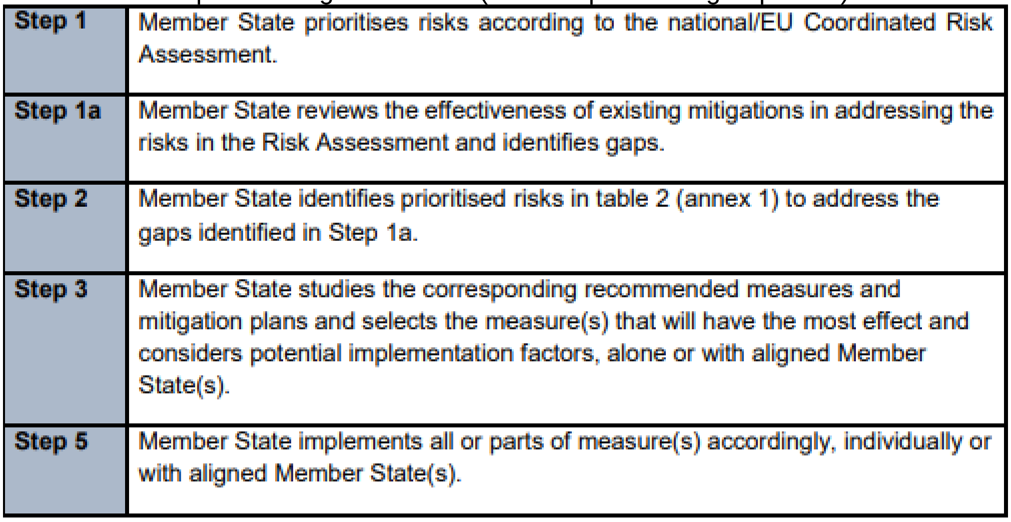

RISKS
may be mitigated by
contribute to the mitigation of
MITIGATING MEASURES
STRATEGIC MEASURES
a) Regulatory powers
b) Third party suppliers
c) Diversification of suppliers
d) Sustainability and diversity of 5G supply and value chain
TECHNICAL MEASURES
a) Network security - baseline measures
b) Network security - 5G specific measures
c) Requirements related to suppliers' processes and equipment
d) Resilience and continuity
enabled, supported or made effective with
enable, assist or improve effectiveness of
SUPPORTING ACTIONS

Figure 9. The EU Toolbox measures and the actions (NIS Cooperations group 2020)

The implementation of the measures is decided by the individual Member State depending on the suitability. Also, it is important to assess the ability to enforce the measure. If the Member State has no ability for enforcing the measure on its own, the cooperation with the other Member States should be discussed. The steps for using the toolbox are presented in Table 4 (NIS Cooperations group 2020).

Table 4. The steps for using the toolbox (NIS Cooperations group 2020)



Step 1	Member State prioritises risks according to the national/EU Coordinated Risk Assessment.
Step 1a	Member State reviews the effectiveness of existing mitigations in addressing the risks in the Risk Assessment and identifies gaps.
Step 2	Member State identifies prioritised risks in table 2 (annex 1) to address the gaps identified in Step 1a.
Step 3	Member State studies the corresponding recommended measures and mitigation plans and selects the measure(s) that will have the most effect and considers potential implementation factors, alone or with aligned Member State(s).
Step 5	Member State implements all or parts of measure(s) accordingly, individually or with aligned Member State(s).

3.6 5G Frequency bands allocated in Finland

5G sub-6GHz frequency bands have been allocated and the operators are listed with the frequency bands in Table 5. Millimeter-wave frequency bands are auctioned partly in the future and n258 (25.1 – 27.5 GHz) is the first mmWave band that is expected to be implemented in Finland.

Table 5. Sub-6 GHz frequency bands allocated by 7.9.2020 (Matkaviestinverkkojen taajuudet ja luvanhaltijat 2020)

OPERATOR	BTS RX FREQ (MHz)	BTS TX FREQ (MHz)
Ålands Telekommunikation Ab	1920.300 - 1940.100 (Åland)	2110.300 - 2130.100 (Åland)
Elisa Corp.	1920.300 - 1940.100 (excluding Åland) 1940.100 - 1959.900 (Åland)	2110.300 - 2130.100 (excluding Åland) 2130.100 - 2149.900 (Åland)
DNA Corp.	1940.100 - 1959.900 (excluding Åland)	2130.100 - 2149.900 (excluding Åland)
Telia Finland Corp.	1959.900 - 1979.700 (excluding Åland) 1959.900 - 1979.700 (Åland)	2149.900 - 2169.700 (excluding Åland) 2149.900 - 2169.700 (Åland)
DNA Corp.	2500.000 - 2520.000	2620.000 - 2640.000

	(excluding Åland)	(excluding Åland)
Telia Finland Corp.	2520.000 - 2545.000 (excluding Åland) 2500.000 - 2505.000 2510.000 - 2540.000 (Åland)	2640.000 - 2665.000 (excluding Åland) 2620.000 - 2625.000 2630.000 - 2660.000 (Åland)
Elisa Corp.	2545.000 - 2570.000 (excluding Åland)	2665.000 - 2690.000 (excluding Åland)
Ålands Telekommunikation Ab	2505.000 - 2510.000 2540.000 - 2570.000 (Åland)	2625.000 - 2630.000 2660.000 - 2690.000 (Åland)
Elisa Corp.	2570.000 - 2620.000 (excluding Åland)	2570.000 - 2620.000 (excluding Åland)
Telia Finland Corp.	3410 - 3480 3600 - 3660 (excluding Åland) 3410 - 3510 (Åland)	3410 - 3480 3600 - 3660 (excluding Åland) 3410 - 3510 (Åland)
Elisa Corp.	3480 - 3540 3660 - 3730 (excluding Åland) 3540 - 3640 (Åland)	3480 - 3540 3660 - 3730 (excluding Åland) 3540 - 3640 (Åland)
DNA Corp.	3540 - 3600 3730 - 3800 (excluding Åland)	3540 - 3600 3730 - 3800 (excluding Åland)
Ålands Telekommunikation Ab	3700 - 3800 (Åland)	3700 - 3800 (Åland)

n258 mmWave band 25.1–27.5 GHz were auctioned, and Elisa Corporation won 25.1–25.9 GHz, Telia Finland Corporation 25.9–26.7 GHz, and DNA Corporation 26.7–27.5 GHz. The representative from Elisa Corporation speculating that mmWave will be on the customer market within the year 2021 (5G-verkon mmWave-taajuusalueet huutokaupattiin suomalaisoperaattoreille 2020).

4 THESIS PROJECT – FREQUENCY SCAN IN THE PORT OF KOTKA

In the thesis project, the research investigations were focused on mobile networking frequency bands. The research was conducted in the port of Kotka, Mussalo, where commissioner i.e., Steveco Ltd., had a problem with transferring the camera data from container cranes to control rooms for real-time monitoring. It was seen that with the older mobile networking or wireless technologies, the upload speed of connections was not high enough for providing real-time monitoring. Hence, the methodology for the thesis included a literature review of the 5G technology, the practical frequency scanning in the port of Kotka, Mussalo and analysis of the results.

4.1 Frequency scanning

In the practical phase of work, the focus was to make measurements in the Steveco Ltd. area to gain a comprehensive set of results in the harbour area. In the measurements planning, XAMK’s 5G FINLOG project leaders were conducting the research for possible scanners to be used. Rohde & Schwarz products were found easy to get for research purposes, and the features included provided a comprehensive set of tools for the measurements. Based on these facts, a R&S PR200 portable monitoring receiver was used as the scanner in the first measurements. After the first measurements, XAMK’s 5G FINLOG project leaders defined the need of second measurements with a different set of scanning tools. After the negotiations with the Rohde & Schwarz representative, R&S®TSME6 scanner and R&S®ROMES4 Drive Test Software was chosen for the second measurements as a good combination of scanning tools.

There are multiple networks deployed in the harbour area of Mussalo. The networks are listed in Table 6.

Table 6. Networks deployed in Mussalo harbour (Steveco Ltd.)

Network	Responsible organization
450 MHz	Edzcom
2.5 GHz (point-to-multipoint)	Nokia
2.6 GHz	Edzcom

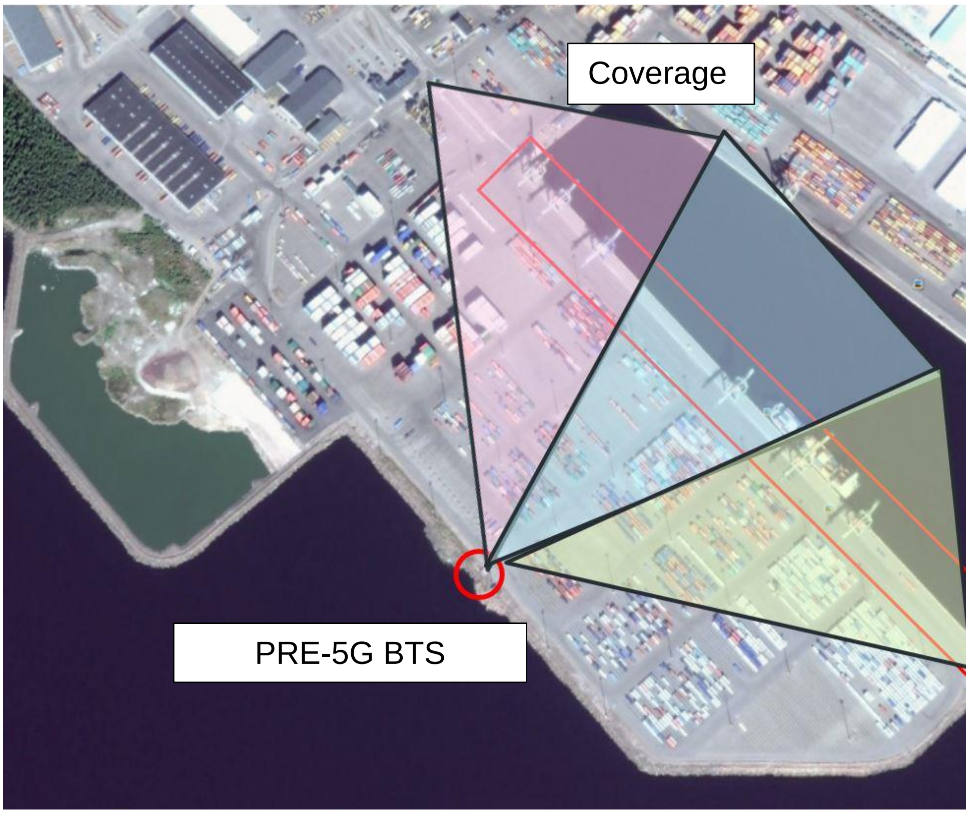


Figure 10. Pre-5G base station (Steveco Ltd.)

Figure 10 depicts the location of pre-5G base station in the port of Kotka, Steveco premises. The coverage is divided into three sectors, which are pointing to the container cranes, where the cameras are deployed. The radio network plan was made for two base stations. Figure 11 illustrates the plan how the container field is covered with two base stations.

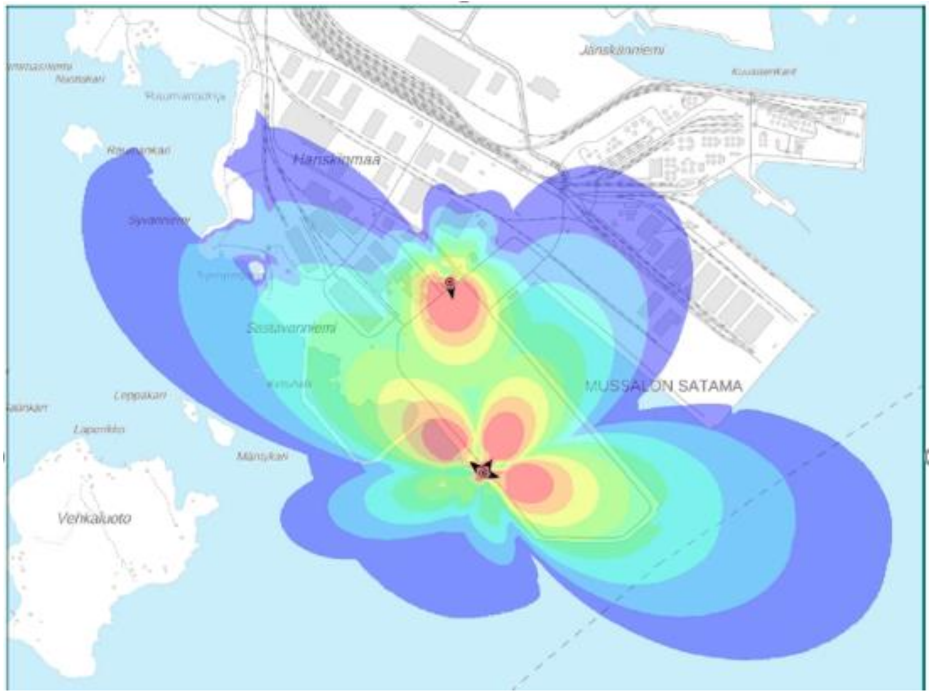


Figure 11. Radio network plan with two base stations (Steveco Ltd.)

4.1.1 R&S®PR200 Portable monitoring receiver

PR200 portable monitoring receiver provides a comprehensive set of tools for signal processing. The main features are PScan, polychrome spectrum and level mapping. PScan is be used for measuring the transmission at a certain frequency area, polychrome spectrum shows the hidden spectrum within the specific frequency area and level mapping creates the map of a certain area with the values of signal strength. The receiver can be found very useful for many different targets, like, interference hunting and radio reconnaissance and surveillance (© Rohde & Schwarz; R&S®PR200 Portable Monitoring Receiver 2020). Multiple different features enable executing the diverse set of measurements. The project features being used were PScan, polychrome spectrum, and level mapping.

Figure 12. R&S®PR200 Portable Monitoring Receiver (© Rohde & Schwarz; R&S®PR200)

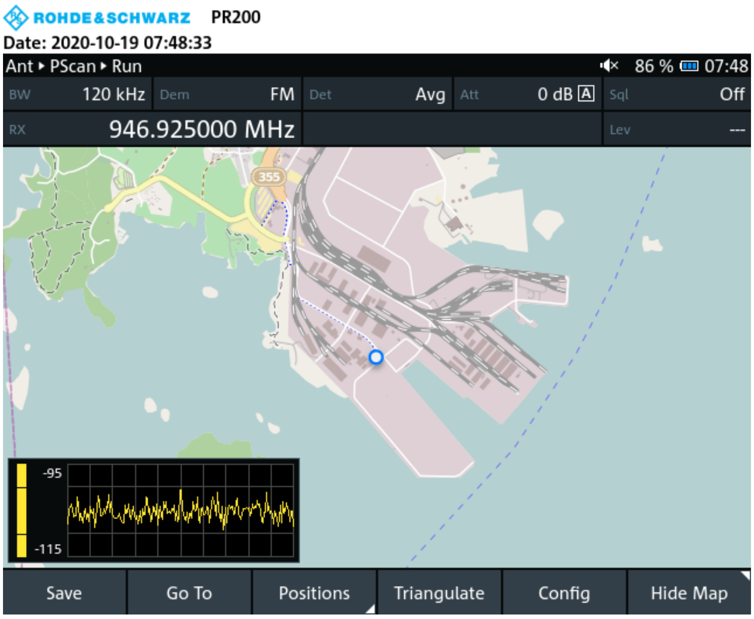
Portable Monitoring Receiver 2020)

The first set of measurements were carried out on 19 October 2020 between 10 am–3 pm. A total of one device was used, and the covered area was the container field. The PScan feature in PR200 portable monitoring receiver showed frequency sweeps in different frequency bands in the first phase of measurements included. The frequencies are listed in Table 7.

Table 7. Frequency bands swept with the scanner.

Frequency band (MHz)
300–700
700–1100
1100–1600
1600–2100
2100–2700
2700–3200
3200–4000
4000–4500
4500–6000

The first image shows the location where the measurements started in the first phase. The frequency sweeps were made on the rooftop of the action centre (Toimintakeskus) in Mussalo as shown in Figure 13.


ROHDE&SCHWARZ PR200

Date: 2020-10-19 07:48:33

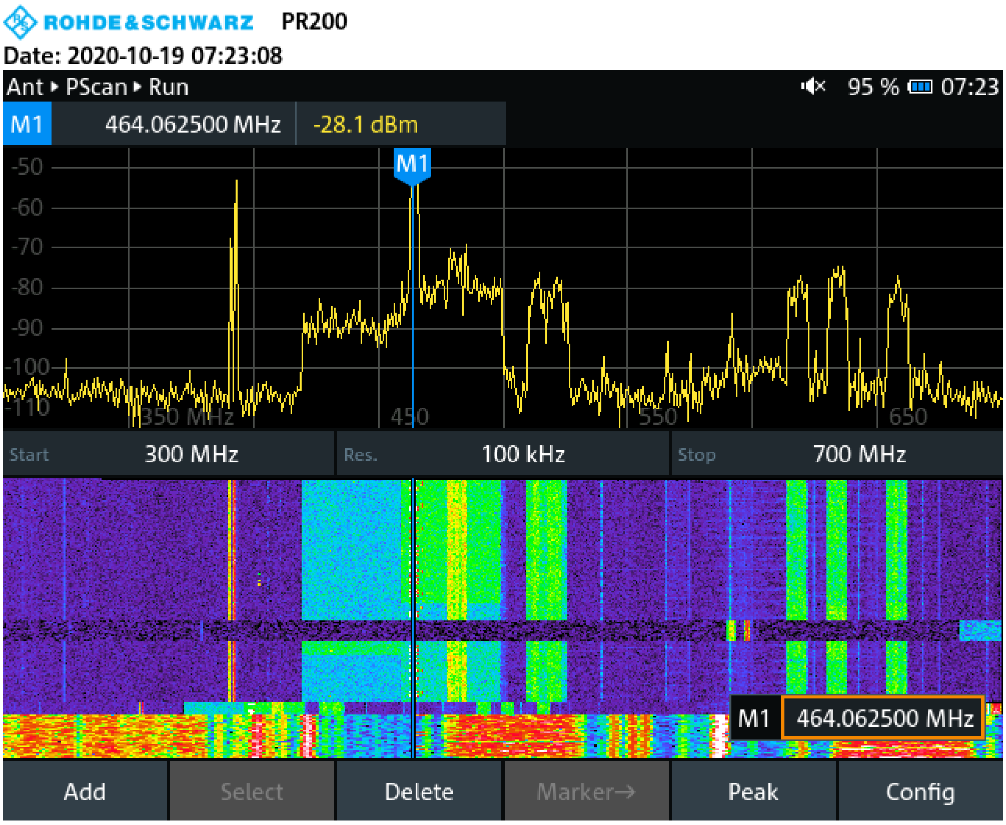
Ant ▸ PScan ▸ Run 86 % 07:48

BW 120 kHz | Dem FM | Det Avg | Att 0 dB A | Sql Off

RX 946.925000 MHz | Lev ---

Figure 13. The location of the measurements in the first phase (R&S®PR200).

The frequency sweeps started with the frequency range from 300 MHz to 700 MHz. The sweeps were made with the PScan feature in the scanner. PScan image is presented in Figure 14.


ROHDE&SCHWARZ PR200

Date: 2020-10-19 07:23:08

Ant ▸ PScan ▸ Run 95 % 07:23

M1 464.062500 MHz -28.1 dBm

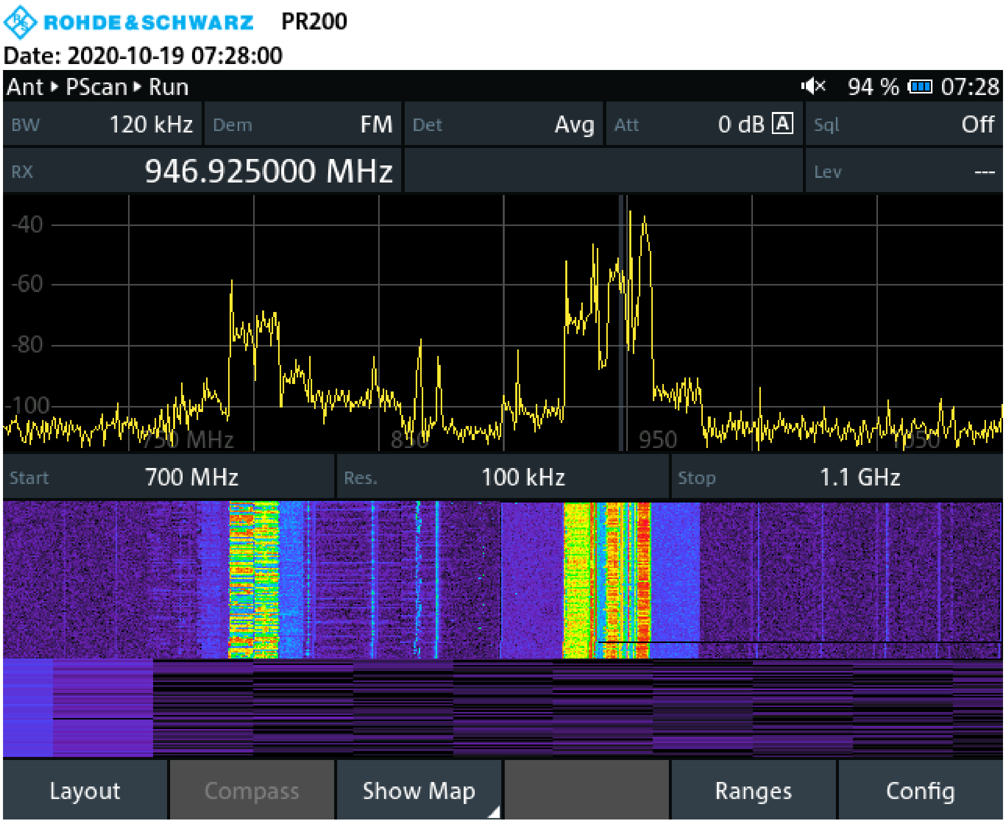
Start 300 MHz | Res. 100 kHz | Stop 700 MHz

M1 464.062500 MHz

Figure 14. The frequency sweep from 300 MHz to 700 MHz.

PScan image from 300 MHz to 700 MHz showed the existing network of 450 MHz. There is one peak between 380 MHz and 395 MHz, which can be caused by different reasons. For example, in this project, mobile phones were found on testing crews' pockets, so the cause can be WLAN, Bluetooth, GPS, etc (Traficom 2020). The next frequency range is from 700 MHz to 1.1 GHz. The image of this frequency sweep is displayed in Figure 15.

,



ROHDE&SCHWARZ PR200

Date: 2020-10-19 07:28:00

Ant ▸ PScan ▸ Run 94 % 07:28

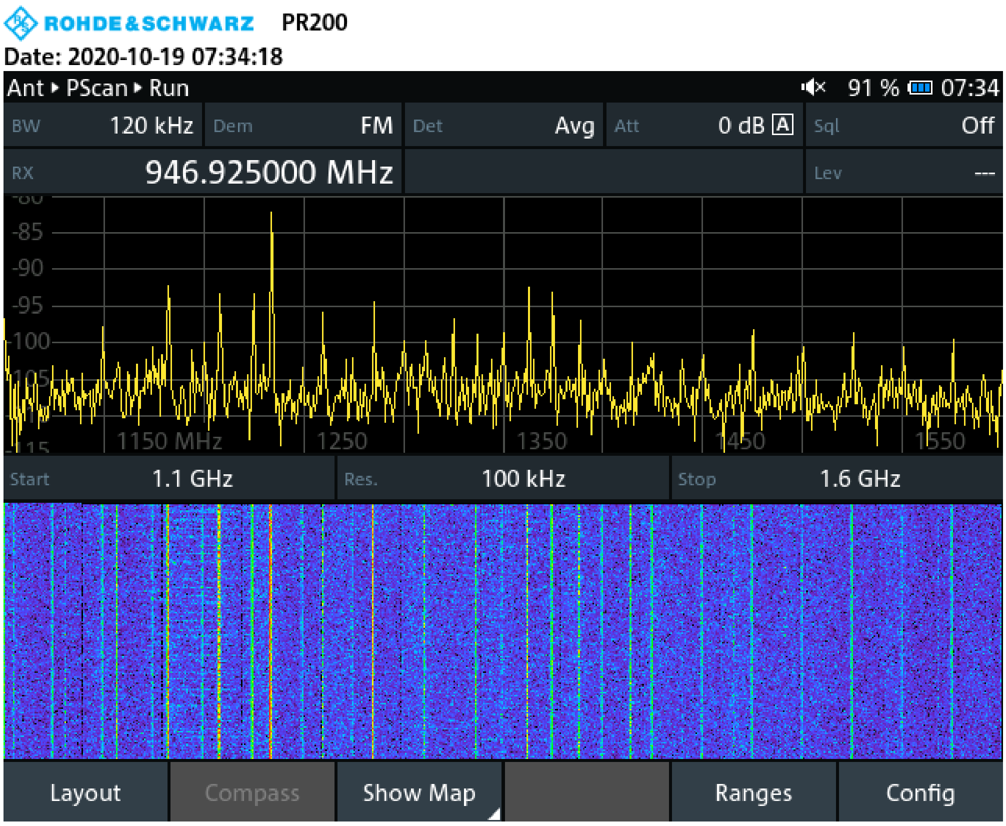
BW 120 kHz | Dem FM | Det Avg | Att 0 dB A | Sql Off

RX 946.925000 MHz | Lev ---

Start 700 MHz | Res. 100 kHz | Stop 1.1 GHz

Figure 15. Frequency sweep from 700 MHz to 1.1 GHz.

The frequency sweep made between 700 MHz and 1.1 GHz shows two peaks, one around 800 MHz and the other one around 900–950 MHz. The 800 MHz frequency can be located to LTE technology band 28 and 44, where the frequency used can be from 700 MHz to 800 MHz. The 900–950 MHz frequency band is used in 2G technologies (GSM). (Traficom 2020).



ROHDE&SCHWARZ PR200
Date: 2020-10-19 07:34:18

Ant ▸ PScan ▸ Run 91 % 07:34

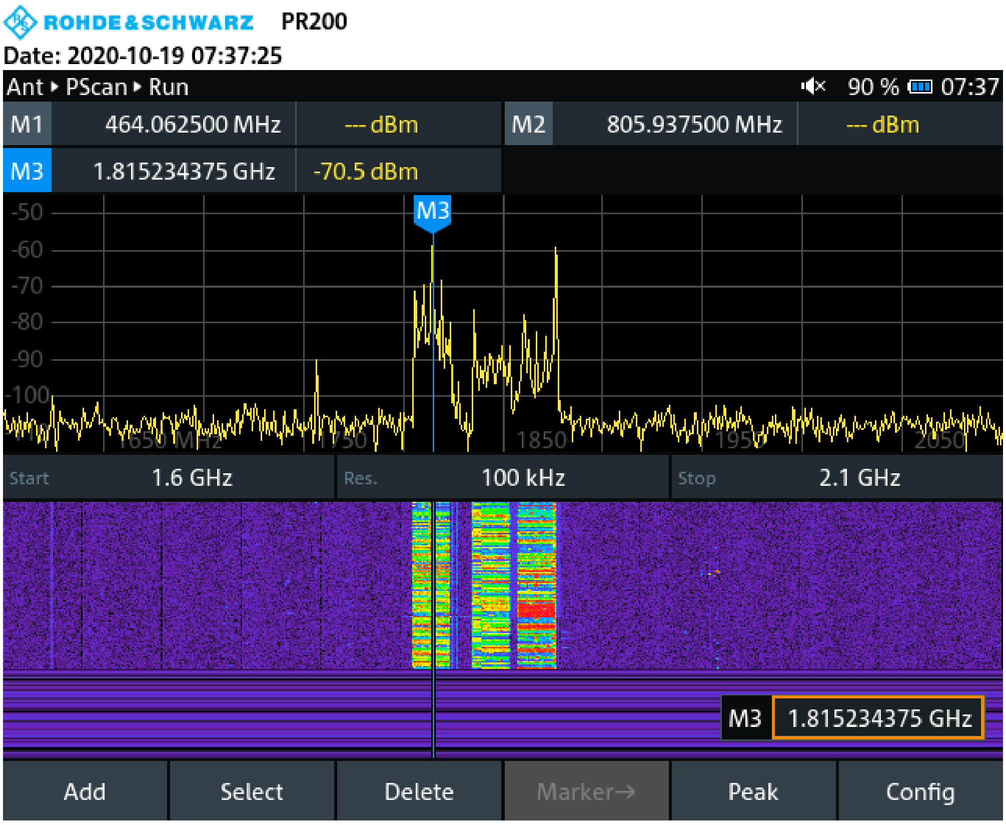
BW 120 kHz
Dem FM
Det Avg
Att 0 dB A
Sql Off

RX 946.925000 MHz
Lev ---

Start 1.1 GHz
Res. 100 kHz
Stop 1.6 GHz

Figure 16. The frequency sweep from 1.1 GHz to 1.6 GHz.

In the frequency sweep between 1.1 GHZ and 1.6 GHz, no specific peaks are visible. However, this frequency band belongs to the L band (500 MHz to 2 GHz), and this band has been used in military telemetry, GPS, 2G (GSM) and amateur radio (Traficom 2020).



ROHDE&SCHWARZ PR200

Date: 2020-10-19 07:37:25

Ant ▸ PScan ▸ Run 90 % 07:37

M1 464.062500 MHz --- dBm

M2 805.937500 MHz --- dBm

M3 1.815234375 GHz -70.5 dBm

Start 1.6 GHz

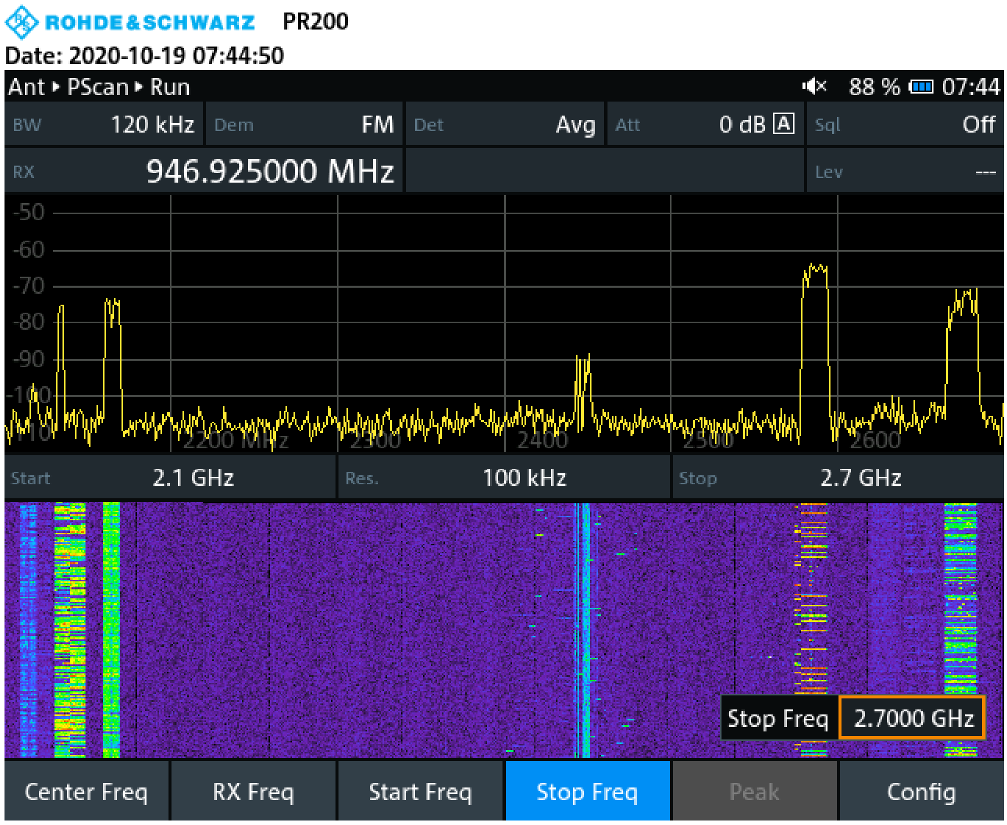
Res. 100 kHz

Stop 2.1 GHz

M3 1.815234375 GHz

Figure 17. Frequency sweep from 1.6 GHz to 2.1 GHz.

As shown in Figure 17, it can be seen that there is traffic between 1.8 GHz and 1.875 GHz. These frequencies belong to the 1800 MHz band and this band has been used in technologies, like GSM, UMTS, LTE or WiMAX. Those operators' networks that are implemented within these frequencies can be found out from the official frequency allocation list. It tells that all current operators (Elisa, Telia and DNA) in Finland have some slots within this frequency area (JM Economics 2018).


ROHDE&SCHWARZ PR200

Date: 2020-10-19 07:44:50

Ant ▸ PScan ▸ Run

88 % 07:44

BW 120 kHz

Dem FM

Det Avg

Att 0 dB A

Sql Off

RX 946.925000 MHz

Lev ---

Start 2.1 GHz

Res. 100 kHz

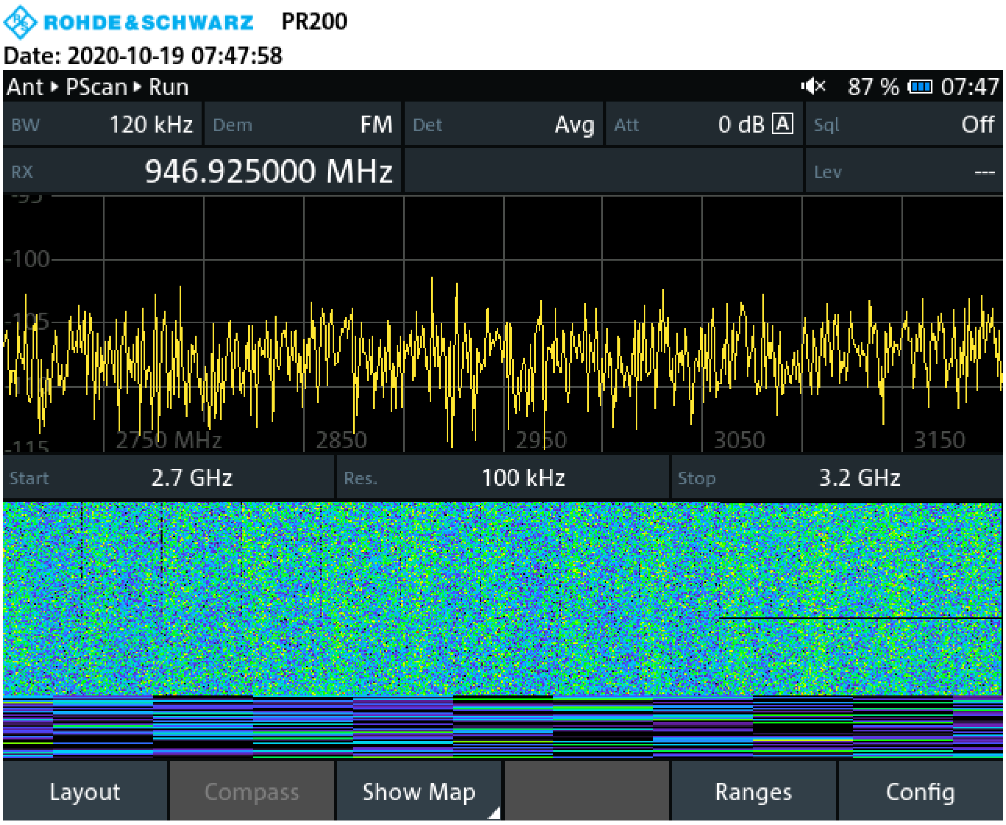
Stop 2.7 GHz

Stop Freq 2.7000 GHz

Figure 18. The frequency sweep from 2.1 GHz to 2.7 GHz.

The frequency sweep conducted belongs to the S-band (2–4 GHz), which is used in weather radars, surface ship radars, communication satellites (Mobile phones, WLAN, Bluetooth, ZigBee, GPS, amateur radio) (Traficom 2020).

As shown in Figure 18, it can be seen that in the beginning there is a small peak, which is belonging to the LTE network within the harbour area. The next one at 2.4 GHz area, which is used in many wireless networking solutions, for example, Bluetooth. Other possible systems using 2.4 GHz frequency are radars and Wi-Fi (802.11b/g/n) (Traficom 2020). The PRE-5G network can be seen in the spectrum in the area of 2.58 GHz. This is the network which has been the main network for testing how 5G could give the wanted performance to camera data transmission from the container cranes to control rooms. In this case, the PRE-5G network is meant to be the test solution and it is implemented by the LTE network with some 5G technologies. The peak at the 2.68 GHz is a pure LTE network operating within the harbour.



ROHDE&SCHWARZ PR200

Date: 2020-10-19 07:47:58

Ant ▸ PScan ▸ Run

BW 120 kHz

Dem FM

Det Avg

Att 0 dB A

Sql Off

RX 946.925000 MHz

Lev ---

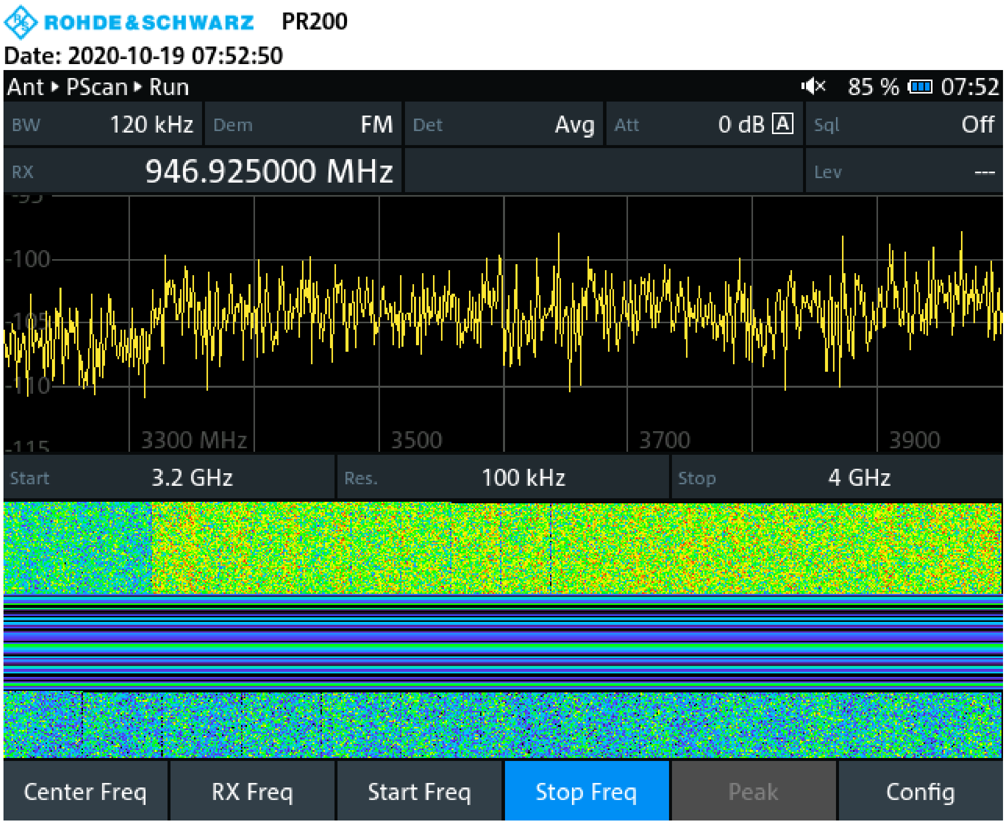
Start 2.7 GHz

Res. 100 kHz

Stop 3.2 GHz

Figure 19. The frequency sweep from 2.7 GHz to 3.2 GHz.

As shown in Figure 19, no existing networks or traffic within the frequencies of 2.7 GHz – 3.2 GHz were found.


ROHDE&SCHWARZ PR200

Date: 2020-10-19 07:52:50

Ant ▸ PScan ▸ Run 85 % 07:52

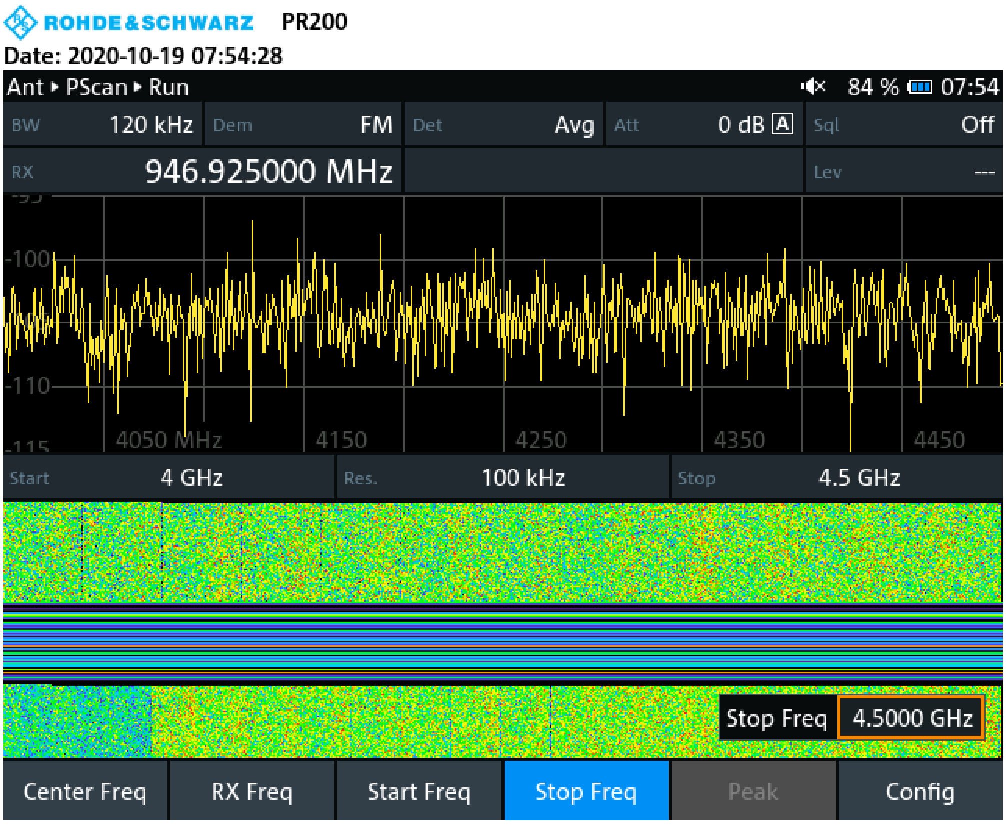
BW 120 kHz Dem FM Det Avg Att 0 dB A Sql Off

RX 946.925000 MHz Lev ---

Start 3.2 GHz Res. 100 kHz Stop 4 GHz

Figure 20. The frequency sweep from 3.2 GHz to 4 GHz.

Those frequencies belong to the S-band, but the C-band starts at 4 GHz. As shown in Figure 20, it can be easily noticed that no existing networks or interfering systems are operating within this area. This band is being auctioned for the 5G NR purposes and will be the first band used in 5G NR networking in the European region. The first 5G network within the port of Kotka will be operating a 3.5 GHz frequency band.



Date: 2020-10-19 07:54:28

BW 120 kHz | Dem FM | Det Avg | Att 0 dB A | Sql Off

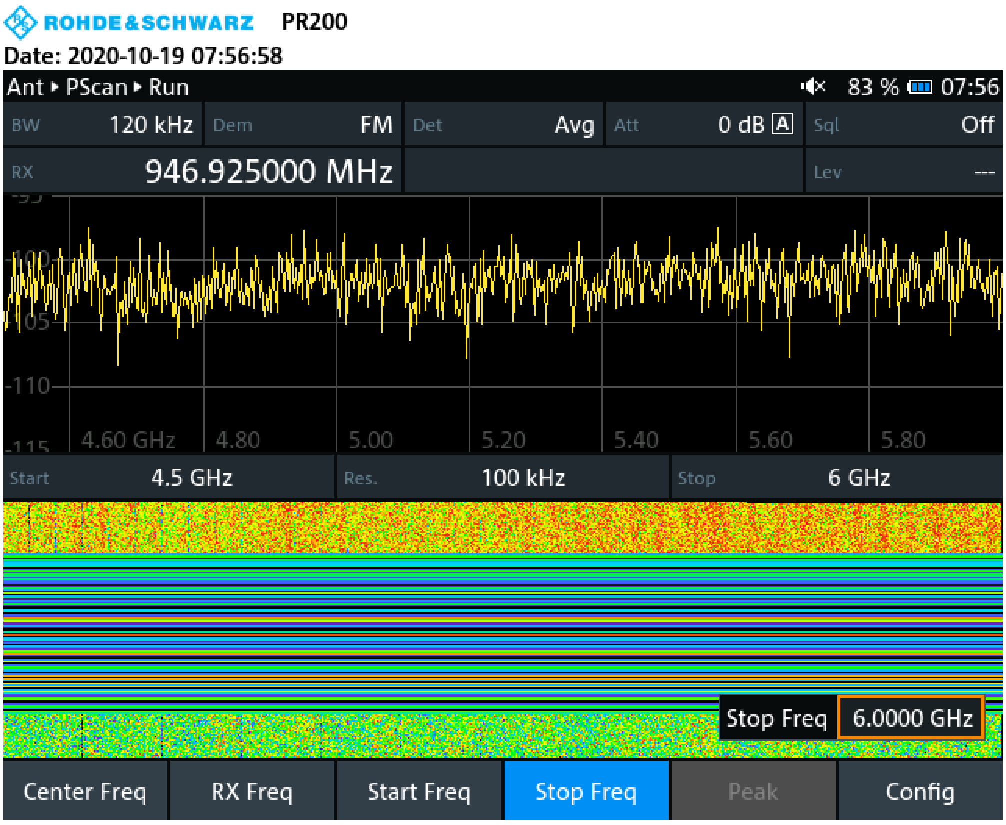
RX 946.925000 MHz | Lev ---

Start 4 GHz | Res. 100 kHz | Stop 4.5 GHz

Stop Freq 4.5000 GHz

Figure 21. The frequency sweep from 4 GHz to 4.5 GHz.

As shown in Figure 21, the frequency sweep reveals that the only traffic traveling is the noise within this frequency area. The frequency 4.2 GHz to 4.4 GHz is used with radio altimeters and wireless avionics intracommunications (WAIC). The frequency of 4.4 GHz to 4.8 GHz is mainly for military use (Traficom 2020).



ROHDE&SCHWARZ PR200
Date: 2020-10-19 07:56:58

Ant ▸ PScan ▸ Run 83 % 07:56

BW 120 kHz | Dem FM | Det Avg | Att 0 dB A | Sql Off

RX 946.925000 MHz | Lev ---

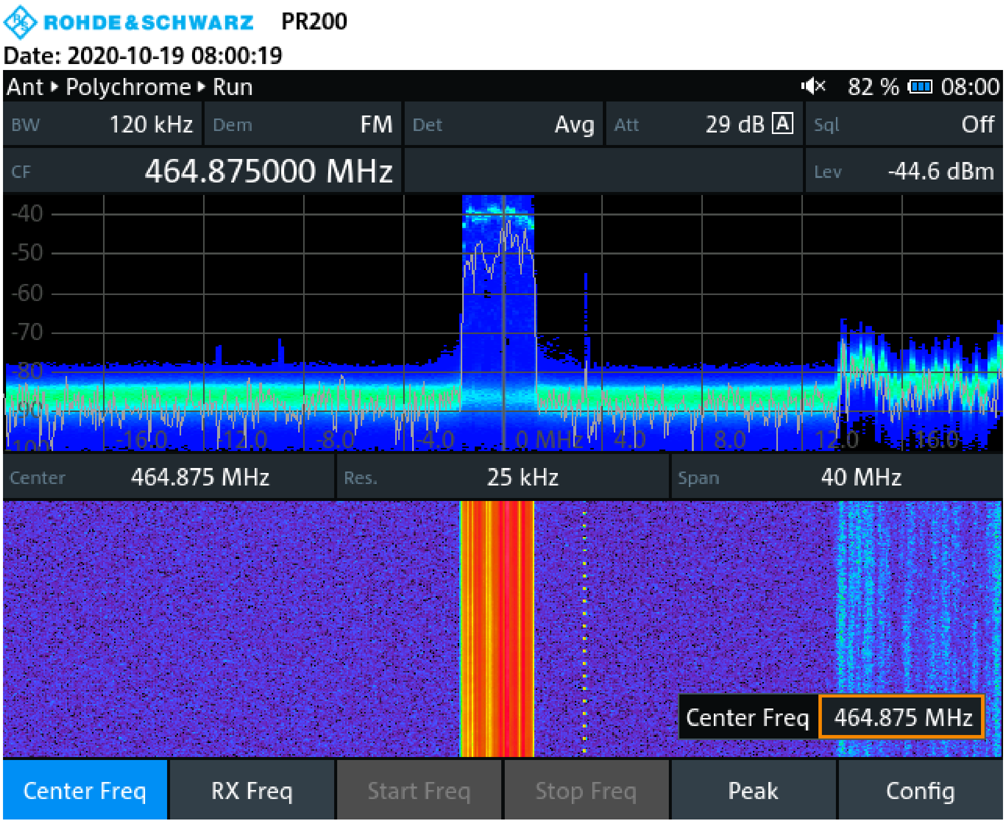
Start 4.5 GHz | Res. 100 kHz | Stop 6 GHz

Stop Freq 6.0000 GHz

Figure 22. The frequency sweep from 4.5 GHz to 6 GHz.

The frequencies between 4.5 GHz and 6 GHz are used for military use, radars, aeronautical radio navigation, radio astronomy, (SRD) Wideband data transmission (WAS/RLAN), earth exploration satellite, meteorological radars, and amateur satellite (Traficom 2020).

Polychrome spectrum feature reveals the hidden signal in a certain frequency range. In this project, one goal was to find out the reason for sudden interferences, and thus this feature is used to identify the hidden signals amongst the frequency bands.


ROHDE&SCHWARZ PR200

Date: 2020-10-19 08:00:19

Ant ▸ Polychrome ▸ Run 82 % 08:00

BW 120 kHz | Dem FM | Det Avg | Att 29 dB A | Sql Off

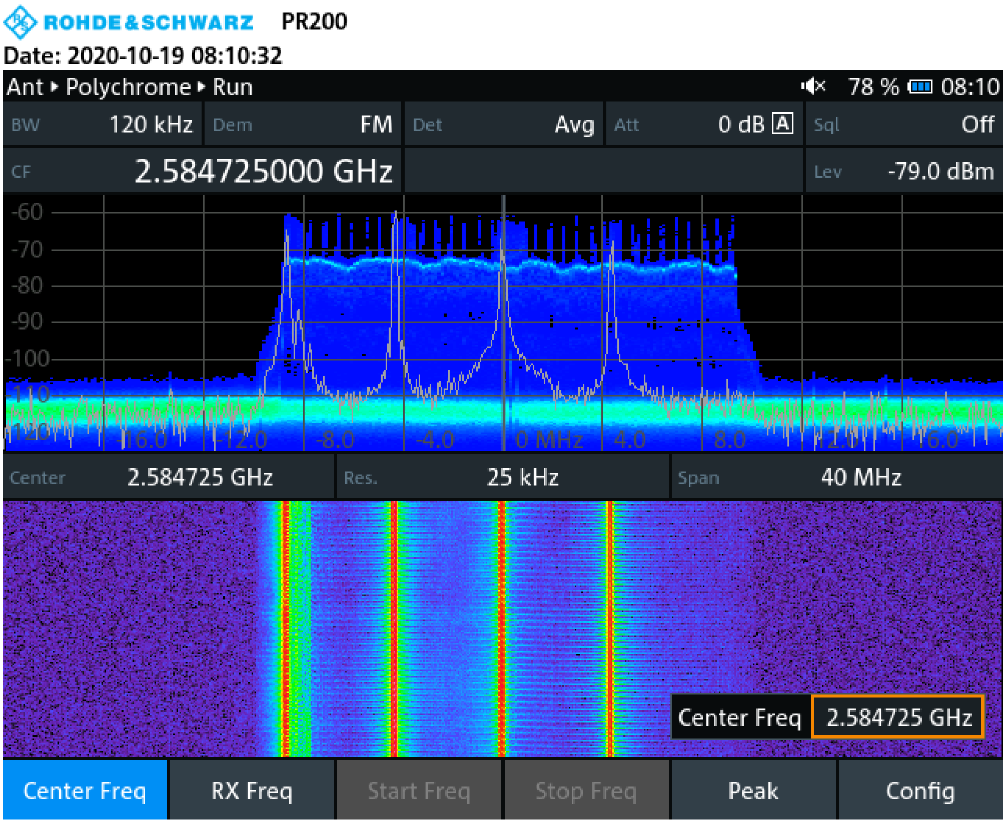
CF 464.875000 MHz | Lev -44.6 dBm

Center 464.875 MHz | Res. 25 kHz | Span 40 MHz

Center Freq 464.875 MHz

Figure 23. Polychrome spectrum in 450 MHz network.

The polychrome spectrum shows the 450 MHz network signal, and the spectrum span is around 4 MHz.


ROHDE&SCHWARZ PR200

Date: 2020-10-19 08:10:32

Ant ▸ Polychrome ▸ Run 78 % 08:10

BW 120 kHz | Dem FM | Det Avg | Att 0 dB A | Sql Off

CF 2.584725000 GHz | Lev -79.0 dBm

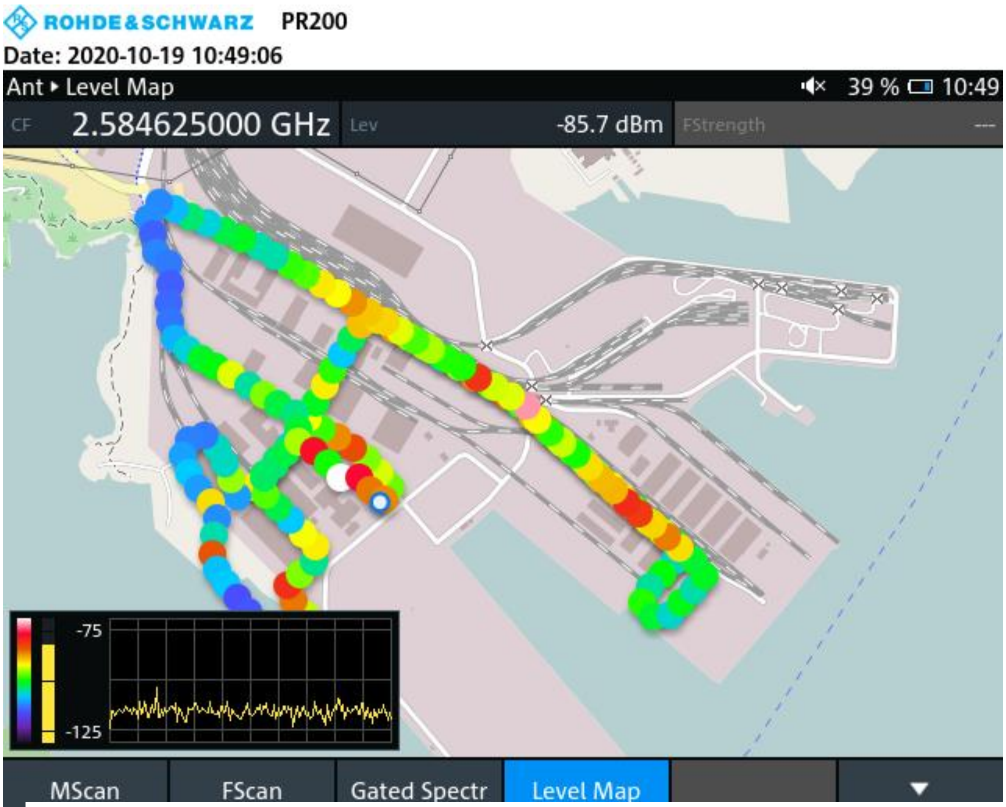
Center 2.584725 GHz | Res. 25 kHz | Span 40 MHz

Center Freq 2.584725 GHz

Figure 24. Polychrome spectrum in 2.6 GHz band.

As shown in Figure 24, it can be analysed how four streams of signals are showing. The frequency span used in this measurement was 40 MHz. The spectrum span is around 16 MHz.

Level mapping in the PR200 scanner creates a map with points, where it is possible to see how efficient the network coverage is. The strength of coverage is printed in different colours. The measurements were made against the known pre-5G network, which is operating in the 2.6GHz area.



ROHDE&SCHWARZ PR200

Date: 2020-10-19 10:49:06

Ant ▸ Level Map

39 % 10:49

CF 2.584625000 GHz Lev -85.7 dBm FStrength ---

Figure 25. Level mapping in the harbour area.

Level mapping for 2.58 GHz depicts how within the port of Kotka most of the areas are covered, and the strength of the spectrum is high enough for the network operations. Most of the spots are between red and light blue and just a few points are violet depicting that the strength of the spectrum is weak.

4.1.2 R&S®TSME6 and R&S®ROMES4

The second measurement was executed a few weeks after the first measurements (29 October 2020). TSME6 scanner and ROMES4 were used as the testing tools. The measurements were carried out using a car (RS-Help 2020). R&S®TSME6 scanner supports simultaneous measurements with different 3GPP technologies and frequency bands without limitations up to 6 GHz. Figure 26 shows the front and rear panels of the scanner (RS-Help 2020).

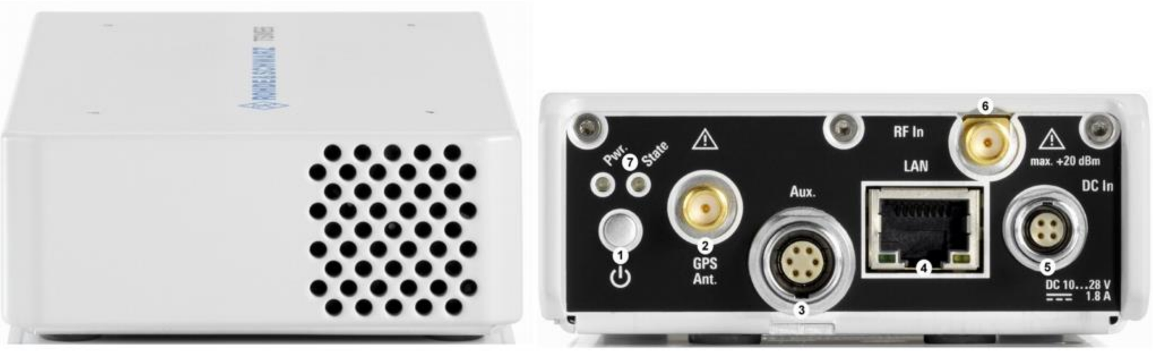


Figure 26. R&S®TSME6 scanner's front and rear panels (*RS-Help* 2020)

R&S®ROMES4 Drive Test Software is made for mobility coverage and QoS measurements in mobile networks (© Rohde & Schwarz; R&S®ROMES4 Drive Test Software 2021). R&S®ROMES4 is the universal software platform used in combination with other test equipment that provides possibilities for multi-purpose measurements, such as coverage and performance measurements, interference identification, and quality analysis in mobile networks (© Rohde & Schwarz; R&S®ROMES4 Drive Test Software 2021). The second measurements were executed to build a comparison between the two different sets of testing equipment. The testing tools used in the second measurement were R&S®TSME6 scanner with the R&S®ROMES4 testing software.

The measurements consisted of the same test cases as in the first measurements, but now there was an opportunity to make the drive tests with equipment made for drive testing. The first measurement was to detect all the possible networks within the harbour area. The testing software had an in-built feature called” Automatic Channel Detection”, which made it easy to find out the operator and in which frequency band the networks are operating. The results are depicted in Figures 27–29.

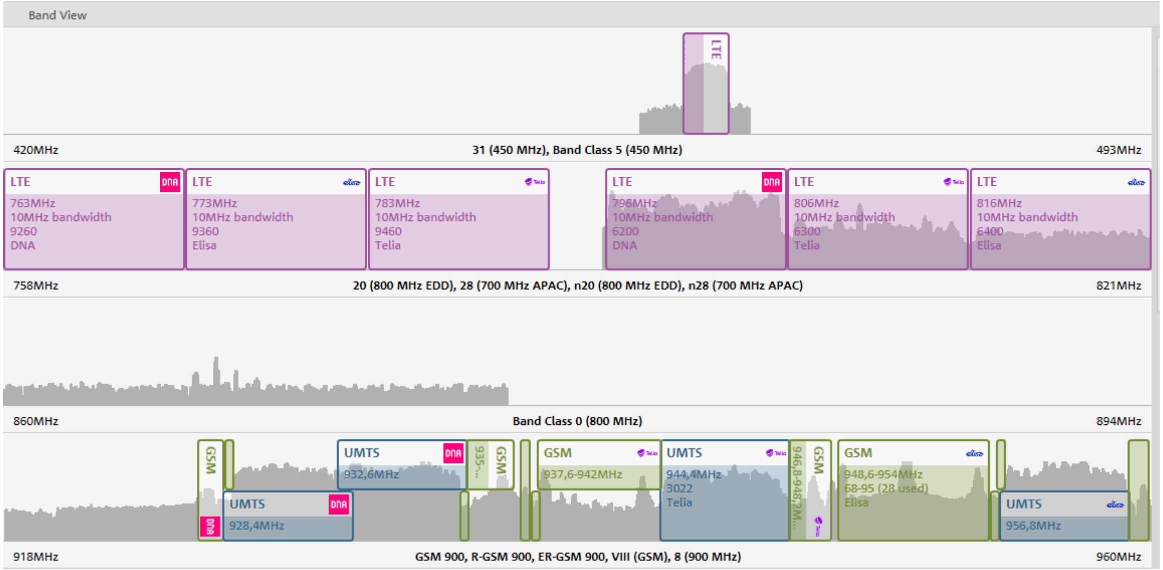

Band View
LTE
420MHz
31 (450 MHz), Band Class 5 (450 MHz)
493MHz
LTE 763MHz 10MHz bandwidth 9260 DNA
LTE 773MHz 10MHz bandwidth 9360 Elisa
LTE 783MHz 10MHz bandwidth 9460 Telia
LTE 796MHz 10MHz bandwidth 6200 DNA
LTE 806MHz 10MHz bandwidth 6300 Telia
LTE 816MHz 10MHz bandwidth 6400 Elisa
758MHz
20 (800 MHz EDD), 28 (700 MHz APAC), n20 (800 MHz EDD), n28 (700 MHz APAC)
821MHz
860MHz
Band Class 0 (800 MHz)
894MHz
GSM
UMTS 932,6MHz
935-...
GSM
GSM 937,6-942MHz
UMTS 944,4MHz 3022 Telia
946,8-948,2M...
GSM
GSM 948,6-954MHz 68-95 (28 used) Elisa
UMTS 928,4MHz
UMTS 956,8MHz
918MHz
GSM 900, R-GSM 900, ER-GSM 900, VIII (GSM), 8 (900 MHz)
960MHz

Figure 27. Automatic Channel Detection 420 – 960 MHz (R&S®ROMES4)

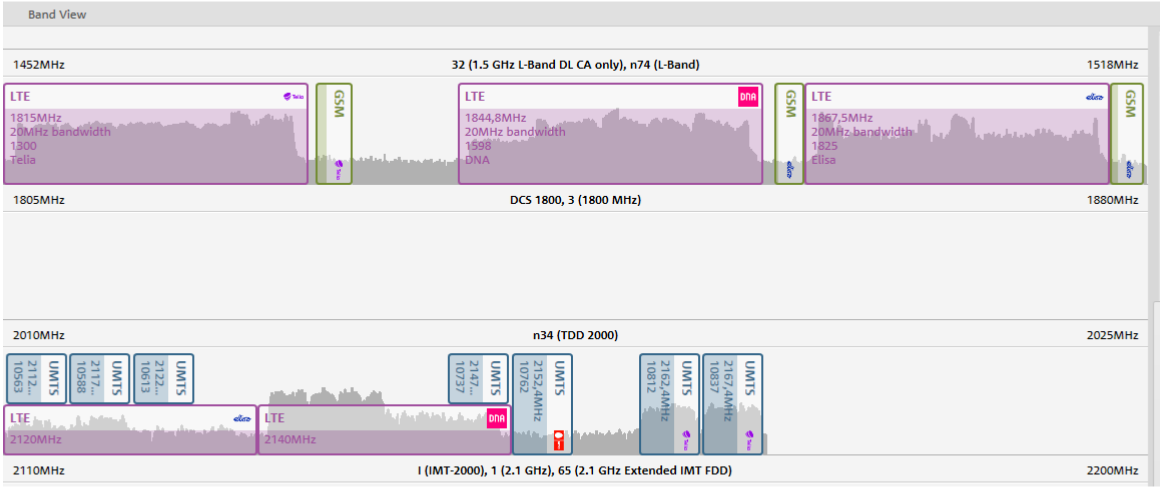


Figure 28. Automatic Channel Detection 1805 – 2200 MHz (R&S®ROMES4)

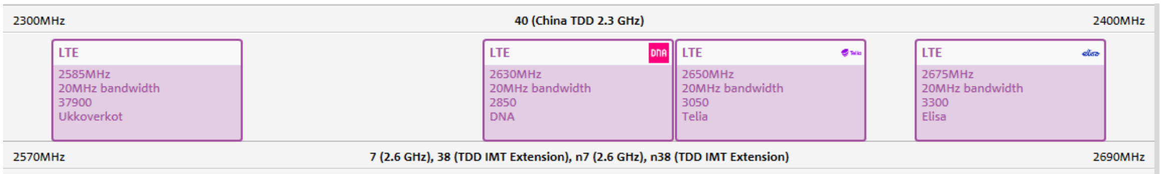

2300MHz
40 (China TDD 2.3 GHz)
2400MHz
LTE 2585MHz 20MHz bandwidth 37900 Ukkoverkot
LTE 2630MHz 20MHz bandwidth 2850 DNA
LTE 2650MHz 20MHz bandwidth 3050 Telia
LTE 2675MHz 20MHz bandwidth 3300 Elisa
2570MHz
7 (2.6 GHz), 38 (TDD IMT Extension), n7 (2.6 GHz), n38 (TDD IMT Extension)
2690MHz

Figure 29. Automatic Channel Detection 2570 – 2690 MHz (R&S®ROMES4)

Figure 29 depicts the pre-5G (LTE 2585 MHz, Ukkoverkot) network, which is the testing network for Steveco Ltd. to have experiences of the upload speed performance. Other networks are just normal LTE networks with all the major operators in Finland (such as, DNA, TELIA, ELISA).

The other feature used in the R&S®ROMES4 software was spectrum scan, where the spectrum of different networks is displayed. The results are depicted in Figures 30–31 below.

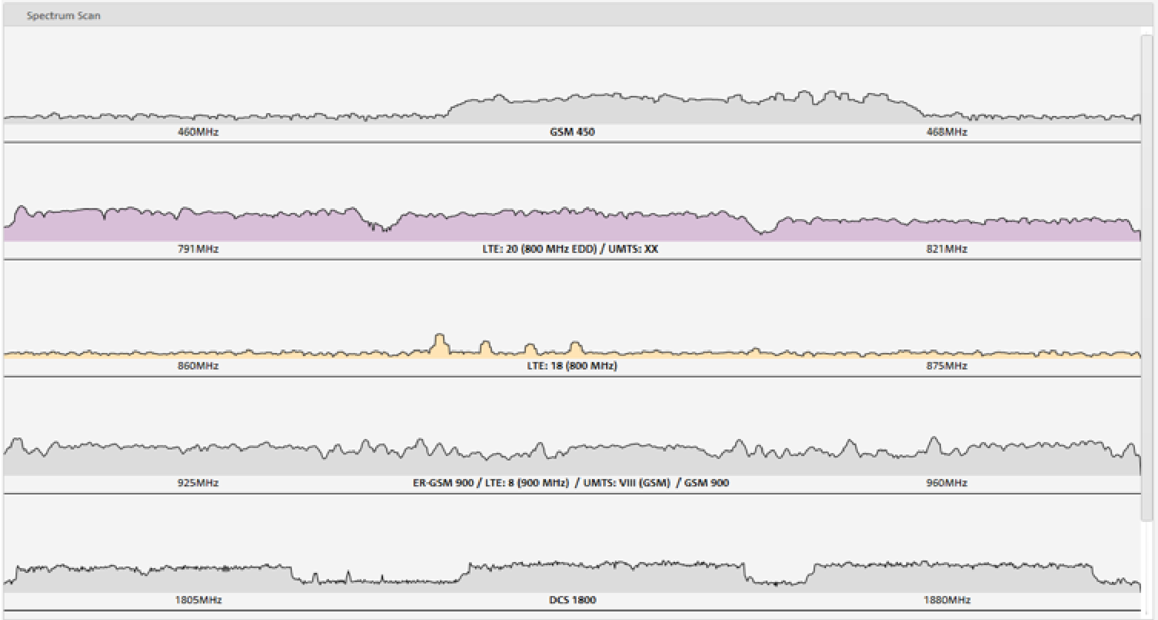


Figure 30. Spectrum Scan (R&S®ROMES4)

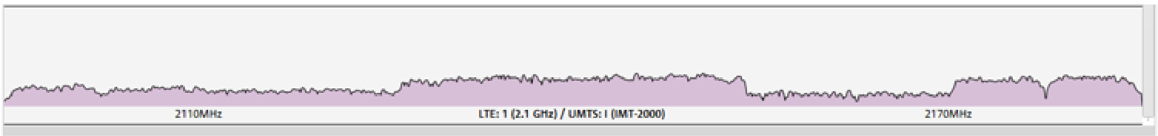


Figure 31. Spectrum Scan (R&S®ROMES4)

Figures 30-31 above illustrate the spectrum of different frequency bands. The information gotten from the “Spectrum Scan” feature can be analyzed for different spectrum oriented research needs. Figure 30-31 shows the operating networks’ spectrum span, and hence, there can be investigations for all possible unexpected spectrums, which are revealed with this feature. This feature can be found in R&S®PR200 Portable Receiving monitor as “PScan”.

The third scenario was the coverage analysis of the pre-5G network within the harbour. The focus in this measurement was identifying the coverage of the network and analysing how well it works at different points. Figure 32 shows how different points are printed in green. Figure 32 also shows what the scales for good and bad coverage values are. The green colour defines the good connection, and the analysis in this scenario is convenient when all the points are printed with one color i.e., green. It is hence asserted that the coverage is good all over the container field and can be declared that the network in the container field is working as intended.

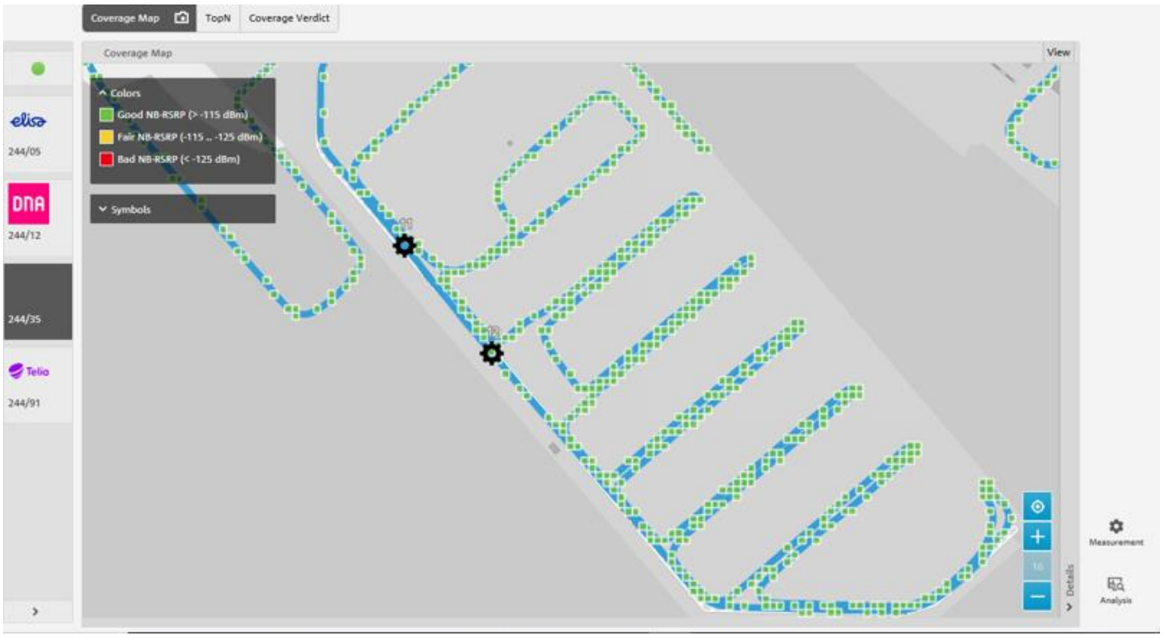


Figure 32. Coverage Analysis for pre-5G network within the container field (R&S®ROMES4)

4.2 Interference incidents

During the ships landing and leaving, interference has been encountered and led to connection losses in the cameras on the container field. This has made safety controlling impossible. In this project, the interference peaks were not identified during the measurements. One reason may be that no ships landed or left during the measurement process. Also, when the second measurement was executed, once again during the measurements, no unexpected peaks were identified. This identifies that the ships followed the prescribed regulations i.e., shutting off the radars when approaching and when leaving the harbour, and powering on the radars again otherwise.

4.3 Software-Defined Monitoring (SDM) for 5G networks

The currently used monitoring systems is equipped with hardwired operational logic when changes require complex configurations or changes in the firmware (Liyanage et al., 2017). Software-defined monitoring is a scheme where the monitoring functions are transferred to the software. SDM framework is a design where monitoring functions are performed in SDN/NFV-based 5G mobile network architectures (Liyanage et al. 2017). The limitations of legacy monitoring systems make the network management more time-consuming and challenging when all the policies and functions are based on physical resources, whereas in SDM the centralized controller is responsible for all the network functions in the network. Current monitoring techniques are lacking interoperability, which makes the network monitoring complex. In SDM the common device standards and single control protocol allow multi-vendor monitoring systems to be implemented. In Table 8 certain differences between legacy systems and SDM are depicted (Liyanage et al. 2017).

Table 8. Legacy monitoring vs. SDM (Liyanage et al. 2017)

Legacy monitoring	SDM
Distributed uncoordinated monitoring	SMD controller is responsible for all monitoring functions in the network
Lack of interoperability and vendor-specific systems	Common device standards and single control protocol allows multi-vendor system implementations
Lack of adaptation	Policies can be changed by software applications
Over-provisioned monitoring mechanism	Mechanisms can be adjusted dynamically according to the demands
Challenges in deployment, updates, and automation	Network management by the centralized controller. Monitoring implemented by software applications enabling easy updates and modifications
Inability to monitor virtualized devices	SDM framework enables monitoring virtualized devices

Software defined monitoring framework implementations are based on 5G SDMN architecture. Figure 33 depicts the basic principle of network monitor framework for 5G SDMN (Liyanage *et al.* 2017).

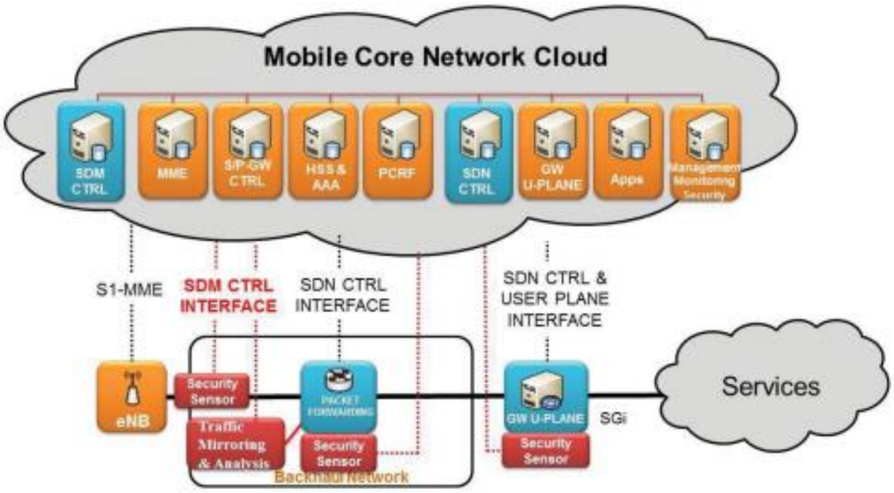


Figure 33. Network monitoring framework for 5G SDMN (Liyanage *et al.* 2017)

4.3.1 **Arista DANZ Monitoring Fabric ™**

In the field of SDM, there are a few manufacturers on the market offering the SDN monitoring solution. In this thesis, the objective was to introduce one SDN monitoring solution by Arista Networks. DANZ Monitoring Fabric (DMF) is the industry’s first network packet broker (NPB) that leverages an SDN-controlled fabric using high-performance, merchant-silicon switches, and industry-standard x86 servers to deploy highly scalable, agile, and flexible network visibility and security solutions (Networks 2020). Based on merchant silicon hardware, DANZ Monitoring Fabric (DMF) provides a scale-out fabric design with integrated analytics and packet recording intelligence (Networks, 2020). The other advantages of DMF are zero-touch fabric operations via DMF controller, fabric modularity, and multi-vendor interoperability (Networks, 2020). Figure 34 shows the architecture of DMF.

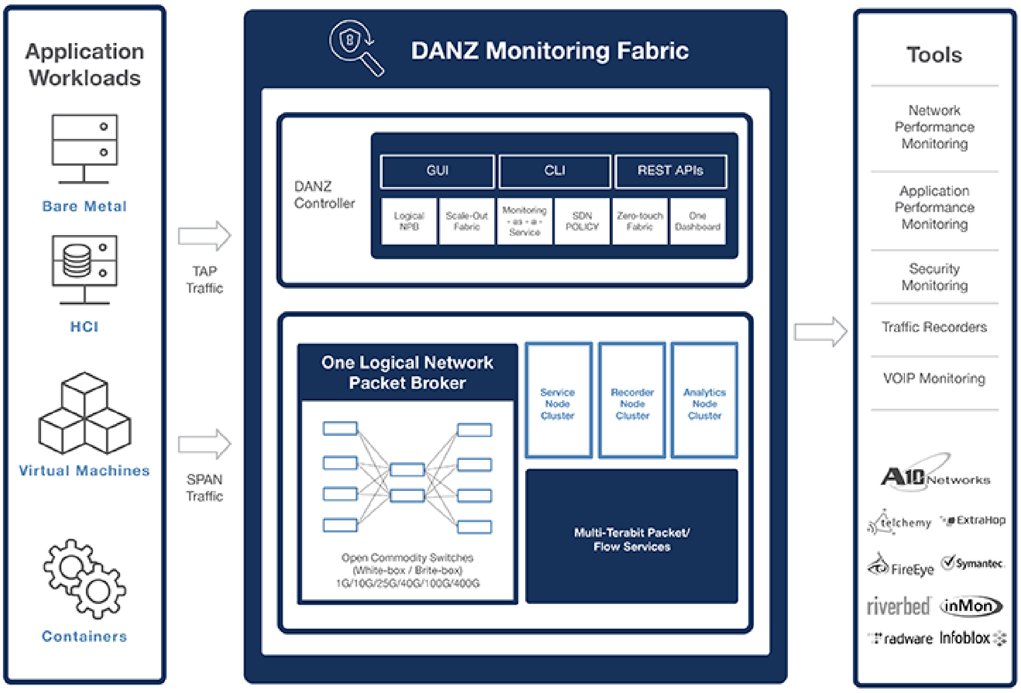
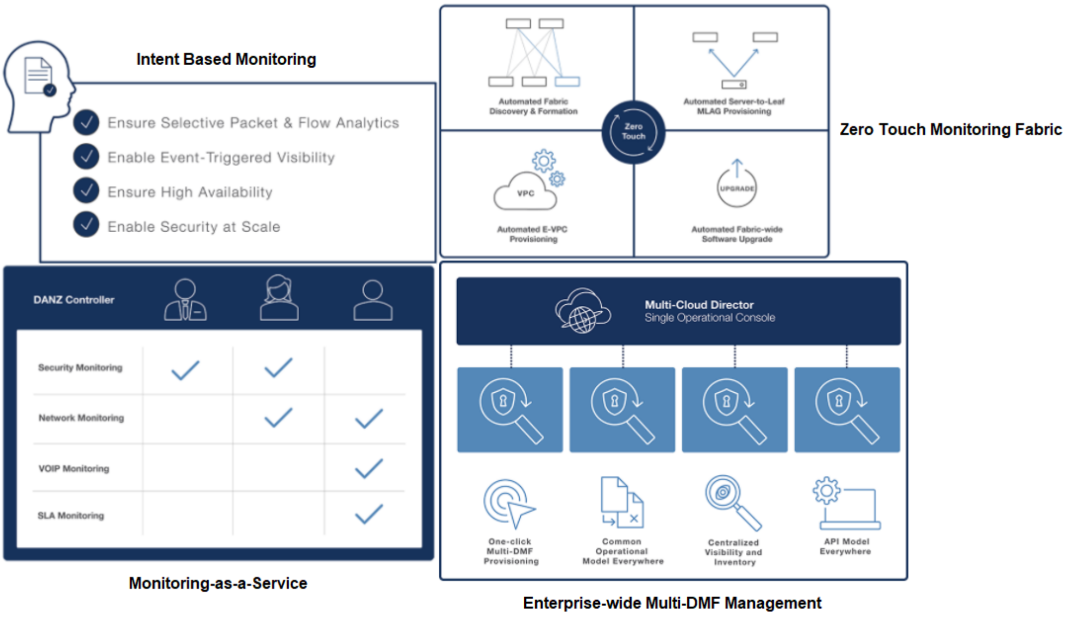


Figure 34. The Architecture of DANZ Monitoring Fabric (Networks 2020)

As shown in Figure 34, Arista DANZ Monitoring Fabric is a solution, which offers a comprehensive set of mechanisms for monitoring the network, with the flexibility in management when the DMF controller controls all the network functions. The features provided for different kind of environments makes the DMF attractive SDN monitoring solution for enterprises. In the port of Kotka, when implementing a 5G network, the monitoring solution should be planned as a part of the network planning. Arista DMF solution could be one alternative because of its scalability and security controls. The security controls enable better traffic monitoring when interference incidents occur in the harbour area (Networks 2020).


Intent Based Monitoring
Ensure Selective Packet & Flow Analytics
Enable Event-Triggered Visibility
Ensure High Availability
Enable Security at Scale
Automated Fabric Discovery & Formation
Automated Server-to-Leaf MLAG Provisioning
Zero Touch
VPC
Automated E-VPC Provisioning
UPGRADE
Automated Fabric-wide Software Upgrade
Zero Touch Monitoring Fabric
Multi-Cloud Director
Single Operational Console
One-click Multi-DMF Provisioning
Common Operational Model Everywhere
Centralized Visibility and Inventory
API Model Everywhere
Enterprise-wide Multi-DMF Management
Monitoring-as-a-Service

DANZ Controller			
Security Monitoring	✓	✓	
Network Monitoring		✓	✓
VOIP Monitoring			✓
SLA Monitoring			✓

Figure 35. Arista Networks DANZ Operations (Networks 2020)

5 CONCLUSIONS

The fifth generation of mobile networking is about to revolutionize the whole paradigm of networking. It is introducing? the concept of “Interconnected World” when devices are increasingly connected to the network and the usage of smart devices is being recognized as an essential part of everyday life. The efficiency in communication reaches an extremely high level but at the same time the flip side of the coin is the lack of security measures in devices connected to the home networks. 5G is introducing numerous different new features and, also technologies, like, millimeter-wave spectrum (mmWave), which is improving the data speeds remarkably, while the high-frequency bands make all the little obstacles big enough from preventing the networks to operate. Another new technology is 5G New Radio (5G NR), which is introducing the OFDMA as the multiple access technology used in uplink/downlink traffic. Beamforming is fully supported, and the efficiency of the network can be enhanced with beamforming when different end-user devices are served with different beams.

Cybersecurity in 5G has been an important aspect when developing the security measures for concepts, like IoT (Internet of Things) and autonomous information systems. The lack of security measures in devices has lately been recognised as a remarkable threat to networking. The manufacturers are launching more devices with smart features but without any appropriate security features and vetting measures. People are buying these devices and machines and interconnecting them to their home networks. Households are although getting more interconnected, which means that they are also getting more exposed and vulnerable to cyber-attacks if the devices do not carry enough security components and services. Cybersecurity is being taken seriously as an important part of future networking regulations. The concept of the EU Toolbox was introduced to develop the plans for cybersecurity issues and risk mitigations. The intention of creating the framework of security measures is to ensure the adequate level of cybersecurity of 5G networks across the EU among Member States (NIS Cooperations group 2020).

During this research, the main project (i.e., XAMK 5G FINLOG) has alternatively been in progress to build a pure 5G network at the port of Kotka, Mussalo during the spring of 2021. This thesis research was carried out in collaboration with the mentioned project, especially the measurement phase, and aims to contribute to the research gaps. The upcoming network is about to operate at the 3.5 GHz frequency band, as opposed to normal 4G networks' spectrum shared between operators with 20 MHz spectrum. In 5G the spectrum shared between operators is 100 MHz. In XAMK 5G FINLOG project, the final spectrum used is 60 MHz, because Russia is operating with the same frequency band (3.6 – 3.8 GHz), and this regulation (ITU Radio Regulations) is valid in areas which are closer to 60 km to the country border (Yle Uutiset 2021). The frequency scanning within the harbour area was executed two times (between 19 October 2020 and 29 October 2020) with two different testing tools. The first one was done by R&S®PR200 and the results revealed that in the harbour area the existing networks were able to be scanned, however, no unexpected traffic or frequencies were observed. The second measurements were executed by R&S®TSME6 scanner and R&S®ROMES4 Drive Test Software and they confirmed the results of the first measurements i.e., only existing networks were found by frequency scanning, without any unexpected results. Thereby, the first research question was answered with the findings that multiple different mobile networks are operating within the harbour area.

Secondly, the reasons for the connection losses in the port of Kotka, especially to the crane cameras, and the likely cause of such incidents was also interesting. During the measurements, no unexpected frequency bands or peaks were found leading to the conclusion that within the harbour area there are no continuous interference issues with mobile networking. One reason for this outcome could also be the lack of ship traffic during the measurements. During the frequency scanning, there were a few ships observed, and those ships did not cause any problem with the camera data transitions. The third research question implores discussion of cybersecurity aspects in mobile networking, especially towards 5G mobile networking. The technologies are evolving and whenever a new feature is being introduced, it also brings up the idea: how to make the feature meet the security requirements for modern-day threats, for example, cyberthreats. New security methods are developed, and services are implemented with enhanced authentication and encryption. At the same time, the tools for attacking the systems and services are developed to be easy-to-use concluding that attackers do not have to be as advanced to commit to cyber-attacks. In this thesis project, the goal was not introducing all the cyber aspects but depicting a few concerning 5G. EU Toolbox was introduced as a major thing in the cybersecurity field, which pertains to the whole EU and its Member States. This can be found as a starting point for more secured connections and services when the continent (EU) has a coordinated approach and steps for implementing the EU toolbox (NIS Cooperations group 2020).

According to the ideas and implementations introduced, the third research area was answered. 5G networking is not ready internationally, let alone nationally. Such is verified by well documented political and security considerations, controversies and identified ‘back doors’ (Peters and Besley 2019), even though the technology is evolving and surely bringing new security methods and implementations over the years. Mobile networking is developed all the time, and when 5G is introduced for customers, at the same time 6G development is in progress. Networking is a concept with no limits. The development process is aiming at a better performance with more capacity and higher speed connections. The thesis work serves as a starting point for 5G networking in the special areas where the wired connections do not serve as a cost-efficient method. The frequency scanning easily reveals the air interface and what frequency bands, and services are operating in different areas. With testing tools, it is easy to locate the possible causes of the interference incidents and create a coverage analysis for maintaining the knowledge if the networks are operating efficiently within the wanted area. The monitoring solutions are the only way for the owner of the property to find out how the network infrastructure is working and if there is any unwanted traffic flowing in the air. Legacy monitoring is always a choice when implementing the monitoring, but SDN-based SDM solutions are recommended as a modern and cost-efficient way to build flexible and multi-purpose monitoring solutions for the enterprises.

The future research could investigate monitoring of more detailed loads of communication traffic. Moreover, longer duration of monitoring and protocol traffic scanning towards the 5G network in collaboration with operators could also add value to the current research. In addition, monitoring of mobile networks in crucial areas, like electrical distribution and water supply centres could give more detailed information on how well the services are secured from unwanted access and breaches.

REFERENCES

© Rohde & Schwarz; R&S®PR200 Portable Monitoring Receiver. 2020.

© Rohde & Schwarz; R&S®ROMES4 Drive Test Software. 2021.

3GPP A Global Initiative. 2021. LTE, 3gpp.org. Available at: https://www.3gpp.org/technologies/keywords-acronyms/98-lte [Accessed 23 January 2021].

5G_Security_Whitepaper_en.pdf. 2015. Available at: https://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf [Accessed: 10 November 2020].

91-04-5g-2.pdf (2016). Available at: https://dl.cdn-anritsu.com/ja-jp/test-measurement/reffiles/About-Anritsu/R_D/Technical/91/91-04-5g-2.pdf [Accessed: 10 November 2020].

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M. & Gurtov, A. 2017. 5G security: Analysis of threats and solutions. IEEE Conference on Standards for Communications and Networking (CSCN). Helsinki: IEEE, 193–199.

Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Ylianttila, M. & Gurtov, A. 2019. Security for 5G and Beyond, IEEE Communications Surveys & Tutorials.

Ahmadi, S. (2019) Chapter 3 - New Radio Access Physical Layer Aspects (Part 1), in Ahmadi, S. (ed.) 5G NR. Academic Press, 285–409.

Al-Dulaimi, A., Wang, X. & I, C.-L. 2018. 5G Networks: Fundamental Requirements, Enabling Technologies, and Operations Management. Hoboken, USA: John Wiley & Sons.

Al-Hazemi, A. M., Al-Mekhlafi, A. A. & Shaddad, R. Q. 2019. Densification of 5G Heterogeneous Cellular Wireless Network Based on Millimeter-Wave

Communication. First International Conference of Intelligent Computing and Engineering (ICOICE), 1–6.

Arrow. no date. What frequency spectrum will 5G technology use and how does this compare to 4G?, Arrow.com. Available at: https://www.arrow.com/en/research-and-events/articles/what-frequency-spectrum-will-5g-technology-use-and-how-does-this-compare-to-4g [Accessed: 10 November 2020].

JMEconomics. 2018. Finland to renew 900 MHz, 1800 MHz and 2100 MHz licences by a beauty contest – JM Economics Oy, 27 September. Available at: https://www.jmeconomics.fi/finland-to-renew-900-mhz-1800-mhz-and-2100-mhz-licences-by-a-beauty-contest/ [Accessed: 31 January 2021].

Electronics Notes. no date. 5G Waveforms: OFDM & Modulation » Electronics Notes. Available at: https://www.electronics-notes.com/articles/connectivity/5g-mobile-wireless-cellular/waveforms-ofdm-modulation.php [Accessed: 10 November 2020].

Electronics Notes. no date. Understanding 5G NR New Radio » Electronics Notes. Available at: https://www.electronics-notes.com/articles/connectivity/5g-mobile-wireless-cellular/5g-nr-new-radio.php [Accessed: 10 November 2020].

The Ericsson Blog. 2017. *Three design principles of 5G New Radio*, *Ericsson.com*. Available at: https://www.ericsson.com/en/blog/2017/8/three-design-principles-of-5g-new-radio [Accessed: 24 January 2021].

European Commission. 2020. Secure 5G networks: the EU toolbox, European Commission - European Commission. Available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_127 [Accessed: 3 January 2021].

Fitzgibbons, L. 2019. What is OFDMA? Definition from WhatIs.com, SearchNetworking. Available at: https://searchnetworking.techtarget.com/definition/orthogonal-frequency-division-multiple-access-OFDMA [Accessed: 24 January 2021].

Ge, X., Tu, S., Mao, G., Wang, C. & Han, T. 2015. 5G Ultra-Dense Cellular Networks, *arXiv:1512.03143 [cs]*. Available at: http://arxiv.org/abs/1512.03143 [Accessed: 10 November 2020].

Hoffmann, T. R. I. 2019. 5G and the Major Cybersecurity Concerns Regarding the Implementation of the Technology - ProQuest. Available at: https://search.proquest.com/openview/8e15ad0d6d20032b8be494f46403d340/1?pq-origsite=gscholar&cbl=18750&diss=y [Accessed: 10 November 2020].

Holma, H., Toskala, A. & Nakamura, T. 2020. 5G Technology: 3GPP New Radio. Newark, UNITED KINGDOM: John Wiley & Sons, Incorporated. Available at: http://ebookcentral.proquest.com/lib/xamk-ebooks/detail.action?docID=5988980 [Accessed: 31 January 2021].

Huang, J., Wang, C., Feng, R., Sun, J., Zhang, W., & Yang, Y. 2017. Multi-Frequency mmWave Massive MIMO Channel Measurements and Characterization for 5G Wireless Communication Systems, IEEE Journal on Selected Areas in Communications, 35(7), 1591–1605.

InDesign-Understanding-mmWave-for-5G-Networks.pdf. no date. Available at: https://www.5gamericas.org/wp-content/uploads/2020/12/InDesign-Understanding-mmWave-for-5G-Networks.pdf [Accessed: 5 January 2021].

IO-TECH. 2020. 5G-verkon mmWave-taajuusalueet huutokaupattiin suomalaisoperaattoreille, io-tech.fi, 8 June. Available at: https://www.io-tech.fi/uutinen/5g-verkon-mmwave-taajuusalueet-huutokaupattiin-suomalaisoperaattoreille/ [Accessed: 4 January 2021].

ISACA. 2019. 5G and AI: A Potentially Potent Combination, ISACA. Available at: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/5g-and-ai-a-potentially-potent-combination [Accessed: 10 November 2020].

Kaspersky.2020. 5G and Cyber security - All You Need to Know. Available at: https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons

[Accessed: 10 November 2020].

Rohde & Schwarz. 2019. Rohde & Schwarz presents new R&S PR200 portable monitoring receiver. Available at: https://www.rohde-schwarz.com/gr/about/news-press/all-news/rohde-schwarz-presents-new-r-s-pr200-portable-monitoring-receiver-press-release-detailpage_229356-718912.html [Accessed: 8 November 2020].

Rohde & Schwarz. 2021. R&S®TSME6 Ultracompact Drive Test Scanner User Manual. Available at: https://www.rohde-schwarz.com/fi/manual/r-s-tsme6-ultracompact-drive-test-scanner-user-manual-manuals-gb1_78701-556097.html [Accessed: 28 December 2020].

Khan, R., Kumar, P., Jayakody, D., & Liyanage, M. 2019. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions, IEEE Communications Surveys & Tutorials.

Liyanage, M., Okwuibe, J., Ahmed, I., Ylianttila, M., Perez, O., Itzazelaia, M., & de Oca, E. 2017. Software Defined Monitoring (SDM) for 5G mobile backhaul networks, IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), Osaka: IEEE, 1–6..

Ma, Y. 2016. A Survey of Distributed Radio Systems. Available at: https://www.cse.wustl.edu/~jain/cse574-16/ftp/dist_rdo/index.html#sec3 [Accessed: 6 January 2021].

Metaswitch. no date. What is Private LTE and Private 5G. Available at: https://www.metaswitch.com/knowledge-center/reference/what-is-private-lte-and-private-5g [Accessed: 10 November 2020].

Networks, A. 2020. DANZ Monitoring Fabric, Arista Networks. Available at: https://www.arista.com/en/products/danz-monitoring-fabric [Accessed: 6 February 2021].

NIS Cooperations Group. 2020. Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, Shaping Europe’s digital future - European Commission. Available at: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures [Accessed: 3 January 2021].

Nokia. 2019. Nokia: Nokia 5G Transformation 7 Streams for success White Paper, OneStore. Available at: https://onestore.nokia.com/asset/206162 [Accessed: 24 January 2021].

Peters, M. A. and Besley, T. 2019. 5G transformational advanced wireless futures, Educational Philosophy and Theory, 0(0), 1–5.

Qualcomm. 2019. How 5G massive MIMO transforms your mobile experiences, Qualcomm. Available at: https://www.qualcomm.com/news/onq/2019/06/20/how-5g-massive-mimo-transforms-your-mobile-experiences [Accessed: 17 March 2021].

Remcomsoftware. 2017. Beamforming Simulations for 5G mmWave and FD MIMO. Available at: https://www.youtube.com/watch?v=uaiNs4JOLbU [Accessed: 2 February 2021].

Rohde & Schwarz. 2020. RS-Help. Available at: https://www.rohde-schwarz.com/webhelp/TSME6_HTML_User_Manual_en/TSME6_HTML_User_Manual_en.htm [Accessed: 28 December 2020].

ScienceDirect. no date. Orthogonal Frequency Division Multiple Access - an overview | ScienceDirect Topics. Available at: https://www.sciencedirect.com/topics/engineering/orthogonal-frequency-division-multiple-access [Accessed: 23 January 2021].

Soldani, D. 2019. 5G and the Future of Security in ICT’, in 2019 29th International Telecommunication Networks and Applications Conference (ITNAC), Auckland, New Zealand: IEEE, 1–8.

Souppaya, M., Cinchonski, J. and Bartock, M. no date. 5G Cybersecurity: Preparing a Secure Evolution to 5G.

Steveco Ltd. no date. Kotka, Mussalo, steveco.fi. Available at: https://www.steveco.fi/en/index/toimipisteet/tphMBmr6K.html [Accessed: 6 March 2021].

Techplayon. no date. 5G/NR - Techplayon. Available at: http://www.techplayon.com/5gnr/ [Accessed: 10 November 2020].

TechRepublic. 2020. 5G and IoT security: Why cybersecurity experts are sounding an alarm, TechRepublic. Available at: https://www.techrepublic.com/article/5g-and-iot-security-why-cybersecurity-experts-are-sounding-an-alarm/ [Accessed: 10 November 2020].

TEOCO. 2021. 5G Radio Network Planning, TEOCO. Available at: https://www.teoco.com/products-services/ran-solutions/planning/5g-planning/ [Accessed: 31 January 2021].

TEOCO. no date. Network Planning Goes 5G, TEOCO. Available at: https://www.teoco.com/blog/network-planning-goes-5g/ [Accessed: 31 January 2021].

Tikhomirov, A., Omelyanchuk, E. and Semenova, A. 2018. Recommended 5G frequency bands evaluation, 5.

Traficom. 2020. RADIO FREQUENCY REGULATION. Available at: https://finlex.fi/data/normit/45948/Radiotaajuusmaarays_4Z2020_englanti.pdf. [Accessed: 4 January 2021].

Traficom. 2021. Matkaviestinverkkojen taajuudet ja luvanhaltijat, Traficom. Available at: /fi/viestinta/viestintaverkot/matkaviestinverkkojen-taajuudet-ja-luvanhaltijat [Accessed: 4 January 2021].

Tripware Inc. 2020. 5G Technology - The Cybersecurity Implications of Widespread, The State of Security. Available at: https://www.tripwire.com/state-of-security/security-data-protection/cybersecurity-implications-5g-technology/ [Accessed: 10 November

2020].

WIlsonAmplifiers. 2021. What is 4G, LTE, 5G and How are They Different?, WilsonAmplifiers.com. Available at: https://www.wilsonamplifiers.com/blog/the-difference-between-4g-lte-and-5g/ [Accessed: 18 March 2021].

Yle Uutiset. 2021. Nopea 5G-mobiiliverkko jää osassa Suomea vain haaveeksi – tukiasemia ei saa rakentaa, koska ne häiritsevät venäläisten yhteyksiä, Yle Uutiset. Available at: https://yle.fi/uutiset/3-11744186 [Accessed: 18 March 2021].