TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Gustav Gretškov 201724IVSB

An Analysis of the Security Shortcomings of 5G Architecture in Non-Terrestrial Networks

Bachelor's thesis

Supervisor: Aleksei Talisainen
MSc
Co-supervisor Toomas Lepikult
PhD

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Gustav Gretškov 201724IVSB

Analüüs 5G arhitektuuri kasutamise nõrkustest maavälistes võrkudes

Bakalaureusetöö

Juhendaja: Aleksei Talisainen
MSc
Kaasjuhendaja: Toomas Lepikult
PhD

Tallinn 2023

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Gustav Gretškov

01.04.2023

Abstract

The contents of this paper are a meta-analysis of the researches available on the various vulnerabilities present in both 5G technology and Non-Terrestrial Networks. It examines the potential solutions and the declared vulnerabilities of the 5G architecture present in the researches and examines them at a combined angle with NTNs, attempting to meld together the disjointed data available on the topics individually, as well as compare potential solutions or remedies to presented issues. The paper focuses on three different vulnerabilities, each targeting a specific major cyber security pillar – confidentiality, integrity, and availability, and presents two possible courses of action in order to mitigiate the threats – analyzing them in the context of NTNs as well as comparing and providing additional insight received by inspecting the solutions together. The aim of doing such is to fill a gap in more readily accessible and analyzed comparisons of 5G and NTN vulnerabilities and solutions, as well as be an example of said process that could be expanded upon.

This thesis is written in English and is 40 pages long, including 6 chapters, 8 figures and 2 tables.

Annotatsioon

Analüüs 5G arhitektuuri kasutamise nõrkustest maavälistes võrkudes

Selle lõputöö sisu on metaanalüüs saadavalolevatest uurimistöödest erinevates 5G ja maavälistes võrkudes (MVV) eksisteerivate nõrkuste kohta. Käesolev töö uurib uurimustes kirjeldatud potensiaalseid lahendusi ja kuulutatud nõrkusi 5G arhitektuuri kohta ja analüüsib neid maaväliste võrkude kontekstis, üritades ühendada saadavalolevat lahutatud informatsiooni, mida võib leida teemade kohta individuaalselt. Sealhulgas võrdleb autor võimalikke abinõusid käsitlevatele probleemidele. Uurimistöö keskendub kolmele erinevale nõrkusele, millest igaüks käsitleb enamasti erinevat küberturbe fundamentaalsammast – konfidentsiaalsus, terviklikkus ja saadavus, ning esitleb kahte võimalikku tegevussuunda ohtude leevendamiseks. Mõlemat suunda analüüsitakse spetsiifiliselt maaväliste võrkude kontekstis ja võrreldakse üksteisega, pakkudes täiendavat arusaama mida on võimalik leida ainult lahendusi koos vaadates. Töö mõte on täita auk kergemini kättesaadavates ja analüüsitud võrdlustes 5G ja MVV nõrkuste ja lahenduste vahel ning olla näide sellest protsessist, mida oleks võimalik laiendada.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 40 leheküljel, 6 peatükki, 8 joonist, 2 tabelit.

List of abbreviations and terms

(D)DoS	(Distributed) Denial of Service
3GPP	3rd Generation Partnership Project
4G LTE	Fourth-generation long-term evolution
5G	Fifth-generation mobile network
DDPG	Deep Deterministiic Policy Gradient
DMM	DDoS Mitigation Model
FR	Fundamental Requirements
GEO	Geostationary Earth Orbit
GPS	Global Positioning System
HAPS	High-altitude Platform System
ICM	Information Collection Module
IoT	Internet of Things
IPM	Information Processing Module
ISO	International Organization for Standardization
MIMO	Multiple-input Multiple-output
MPM	Model Prediction Module
NB-IoT	Narrowband IoT
NFV	Network Function Virtualization
NGMN	Next Generation Mobile Networks
NTN	Non-Terrestrial Network
QoS	Quality of Service
SATCOM	Satellite-based Communications
SDN	Software-defined Networking
SDSN	Software-defined Satellite Network
SR	Systematic Review
STZ	Security Trust Zone
TAM	Topology Awareness Module
UAV	Unmanned Aerial Vehicle
VNF	Virtualized Network Function

Table of Contents

List of Figures

List of Tables

1 Introduction

Chapter 1.1 outlines some background on NTNs and 5G with historical references to the relevance. Chapter 1.2 provides an overview of the security challenges handled in this paper posed by those systems. Chapter 1.3 defines the aim and considerations taken in this analysis. Chapter 1.4 focuses on the limitations arising from the scope of the paper and chapter 1.5 outlines its structure.

1.1 Non-Terrestrial Networks and 5G

Figure 1 depicts the various types of NTNs, represented and categorized based on type and altitude.

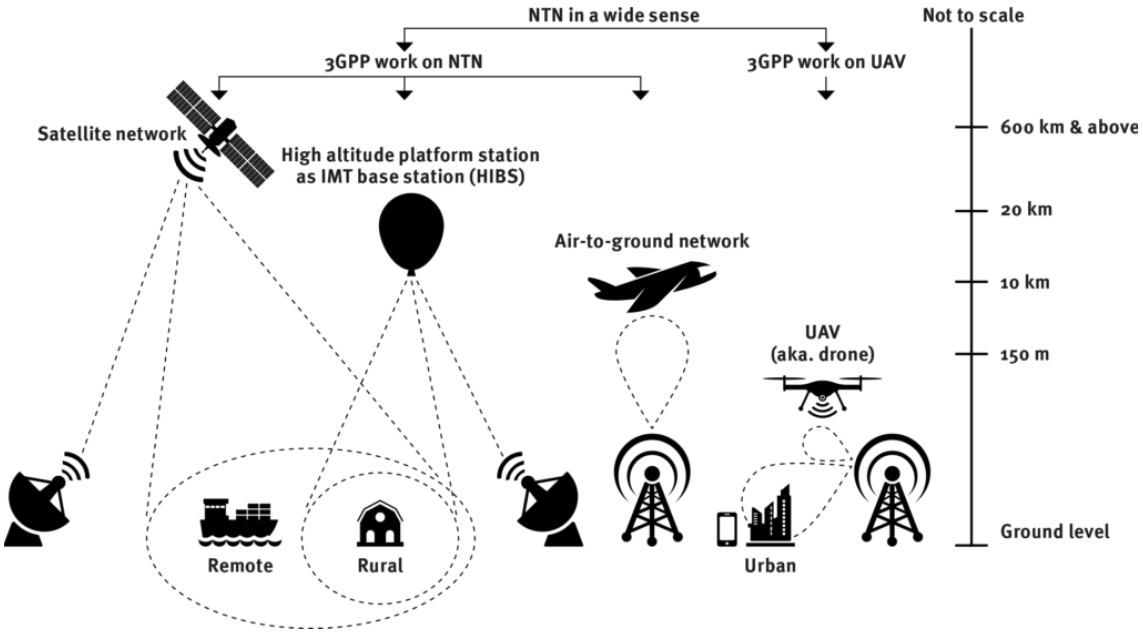

Figure 1. Types of Non-Terrestrial Networks [21]

The main need for Non-Terrestrial Networks (NTN) came from a significant downside of one of the most prevalent types of wireless communication – TV signals. As they only travel in straight lines, TV signals tended to trail off into space instead of following the planet's curve or would get blocked off by mountains or structures. The logistical challenge of setting up telephone wires over long distances was also an issue that was

overcome by satellites – their nature allowing for much more clear and reliable communications across the globe given a sufficient enough network. For the last half of a century, satellite-based communications (SATCOMs), along with other forms of NTNs to a lesser degree, have been a major part of daily lives in a large variety of fields. The general cost of these networks over that time however [1] has largely confined their use to large-scale projects such as weather forecasting, radio broadcasting, the Global Positioning System (GPS), and military communications. 5G itself is a global wireless standard that directly follows from 4G, specifically designed to bring connectivity between virtually any machine possible, therefore heavily supporting both the advent of IoT as well as distributing network services more universally to people across the globe. According to Next Generation Mobile Networks (NGMN), 5G is also built for lifeline communications, sensor networks, high-altitude video surveillance, and even world-reaching broadcast services [5] .

1.2 Overview of the problem

As outlined in the previous chapter, the sheer scale and cost of NTNs restricted their use to fairly major fields of service that affect countless amounts of people per physical device. Despite some of these being clearly more sensitive than the others, the sheer scale and cost of these systems as well as their ever-growing importance leads to NTN security being increasingly more important. The urgency of developing more secure NTNs is furthermore increased by the pioneering of internet coverage through satellites into more rural areas and for a generally wider public that otherwise does not have reliable access to it by governments such as the EU and companies such as SpaceX[2] . With ever-increasing coverage and prevalence comes a proportional increase in the amount of interested malicious actors. Up until this day, attacks on NTN networks have been relatively sparse, though we have already seen a slow trend of it becoming to shift, particularly with the war in Ukraine bringing in more motivated actors on both sides to help the war effort through coordinated cyberattacks on infrastructure [3] . According to the CyberSat advisory board, the biggest satellite security event, the current security measures in place are vastly insufficient for the impending attacks that are only growing more likely due to the ever-increasing Internet of Things (IoT) 5G eco-system [4] .

After exploring various already existing research papers on similar topics about NTN security and 5G (generally separately), the author of this paper has decided to focus on the following security vulnerabilities in current thesis. [20] , [22]

1. Due to the exponential increase in network-capable devices as a result of IoT, Denial of Service (DOS) attacks are already becoming much more potent and NGMN warns that the advent of 5G will bring forth several dangerous types of DOS attacks against network infrastructure [6] .

2. 5G's support for network slicing brings with itself a host of new challenges. Network slicing allows for the same physical infrastructure to be capable of providing for a range of different requirements based on the target of the service through a network function virtualization (NFV) which utilizes a set of virtual network functions (VNFs) for every different 'slice'. [7] The largest concern this feature raises is proper slice separation that would be able to prevent threat actors from accessing slices they are not authorized to. [8]

3. A key physical layer technology used in 5G that is already being adopted into NTNs is massive multiple-input multiple-output (MIMO). As all the vulnerabilities, it will be discussed more in depth later in the thesis, though one of the main weaknesses of this approach is an attacker potentially contaminating legitimate users' pilot transmissions which are used to ensure that data is transferred to the correct person [9] .

1.3 Formulation of the assignment

The aim of this paper is to condense the resources on several key vulnerabilities and issues in adopting 5G into NTNs into one single paper as well as analyse the different solutions proposed with a specific emphasis on their effect in the unique nature of NTNs as there is still a significant lack in such resources even by the 3rd Generation Partnership Project (3GPP) itself. In the case of every vulnerability, the following facets of any given solution will be considered.

1. The cost of implementing the solution. With the ever-increasing miniaturization of physical hardware and progress of technology leading to a decreased cost and therefore a decrease in the barrier of entry into NTNs, special care must be taken when considering the cost of a potential solution as NTNs expand into the more general market and a proposed solution being considered too expensive would dissuade it from being implemented.

2. The solution's effect on the general performance of the system. As NTNs are key to providing communication and network infrastructure in more distant areas as well as during crisis or other life vital operations, it is critical that their performance stay consistent, reliable, and as low-latency as possible.

3. Various other factors that depend on the unique vulnerability at hand. These will be elaborated on more in the paper when discussing them, and also serves as a catch-all point to include other advantages or disadvantages that a solution may offer. It is paramount that a comprehensive overview of the complications and benefits of any given approach are brought up regardless of whether or not they fit into a classification.

1.4 Limitations

The sheer scale of the paper requires that some limitations are put into place. There exist a myriad of vulnerabilities in the implementation of 5G into NTNs, and this paper does not cover all of them but decides to focus on three of some of the biggest complications that arise from the process of integration. The same can also be said for the solutions to those complications, though care has been taken to reasonably cover as many solutions as possible while remaining thorough.

The nature of this thesis also prohibits any sort of experimental output due to the expensive hardware described. It is mainly a meta-analysis focusing on compressing the available information and providing some readily accessible insight into the pros and cons of any given solution.

1.5 Division of chapters

Chapter 2 provides pivotal background information on the concept of NTNs and their workings. It also provides an overview of 5G and some of its most significant features, particularly those that are relevant to the paper at hand. It also has a specific subchapter for every vulnerability that is discussed in this paper, explaining its workings and relevance. Chapter 3 elaborates on the methodology of the paper and its necessity, bringing some understanding of the research already done in similar topics. Chapter 4 comes back to the vulnerabilities mentioned in the previous chapters and instead focuses on the potential solutions as well as an analysis of each and every solution. Chapter 5 highlights the potential and requirement for future research in the field, followed by a conclusive final summary in Chapter 6.

2 Background

Chapter 2.1 and its sub-chapters provide and outline of NTNs and 5G respectively – giving some insight into their history, structure, and relevance. Chapter 2.2 provides an in-depth overview of each of the vulnerabilities under analysis in this paper with its respective sub-chapters.

2.1 5G and NTN Background

The advances in 5G standards have made it more possible than ever to integrate NTNs into a fully fledged, standardized, and interoperable wireless network that stretches across the entirety of the world. The main use cases for the technology are brought out as additional backhaul connectivity options, multi-connectivity, network resilience, critical sensor monitoring and crisis/life-impacting operations communications, including both military and civilian. [5]

2.1.1 Non-Terrestrial Networks

NTN itself as a term is somewhat new, as before that the more prevalent term was SATCOM due to the overwhelming majority of NTN being solely in that realm. As satellites used to be prohibitively expensive to deploy, they needed to have an extremely long life-cycle and cover as much of the planet as possible per satellite. As such, latency was not considered as much of an issue and the majority of satellites launched had a Geostationary Earth Orbit (GEO), being high enough to cover a wide area and simultaneously stay hovering over the same landmass. The latency of such systems by nature limited their use-cases, though they were still used across a number of different applications such as weather (Starting with Tiros-1), communications (Starting with Telstar-1 and moving on with the Intelsat consortium), and imagery (Starting with

Landsat). Only in the year 1994 did the first GPS constellation become operational, and despite an explosion of the amount of satellites in the Earth's orbit leading to over a 1000 by the year 2012, the first private orbital launch site was finished in the year 2017. Ever since then, the leaps in technology have led to small satellites being affordable enough to launch even for relatively small enterprises and individuals, both physical and legal – such as TalTech's student satellites called KOIT and HÄMARIK. [10] [11]

NTNs themselves generally consist of several major components:

1. A non-terrestrial device or vehicle (such as a satellite)
2. A terrestrial endpoint (such as a smartphone)
3. A feeder link connecting the NTN to the terrestrial network
4. A service link between terrestrial and non-terrestrial devices

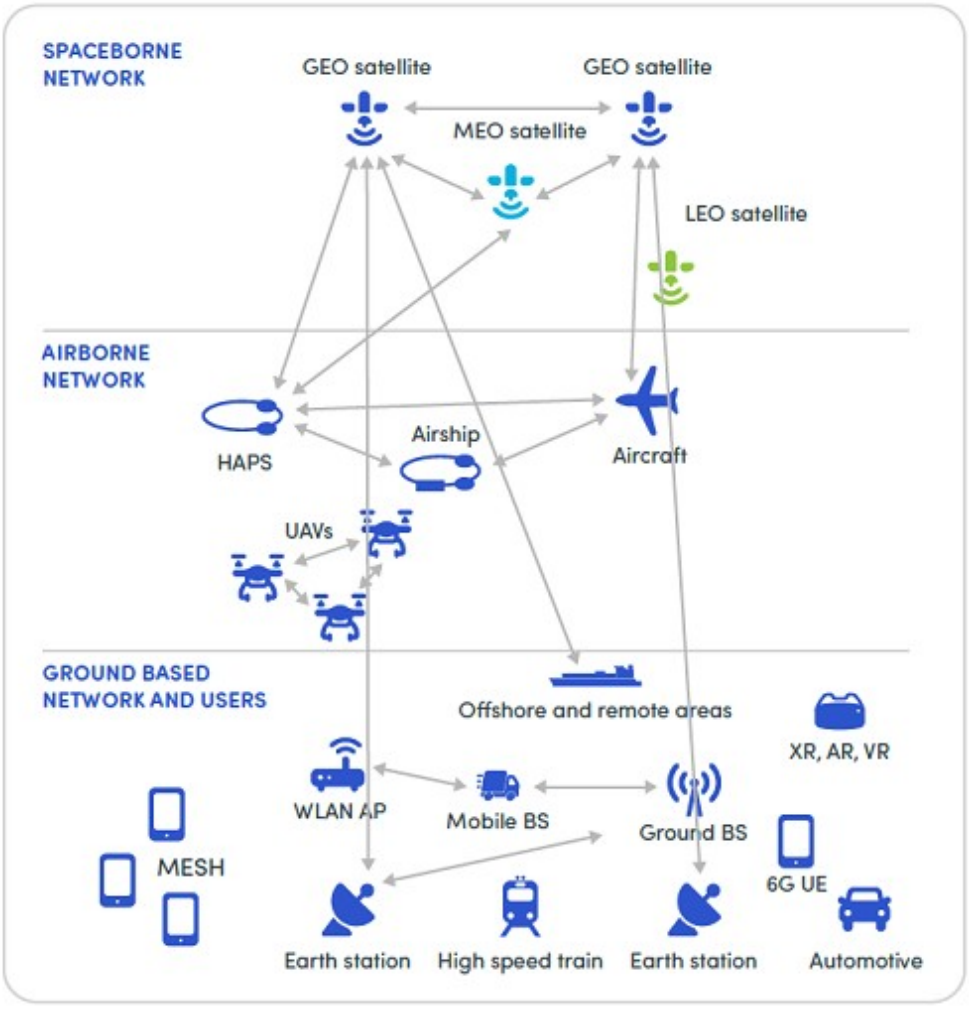

Figure 2. Example of NTNs (upper two rows) [41]

The easiest way to categorize them would be through the non-terrestrial device or vehicle used, resulting in three main types:

1. Satellites, which are higher than the other two and whose purpose depends heavily on the altitude they rest at, ranging from a large variety of different altitudes.

2. Unmanned aerial vehicles (UAVs), which fly the lowest of the three mentioned types, generally providing a broadband link between the devices

3. High-altitude platform systems (HAPS) – These hit a point between the height of the UAVs and satellites, though they are still a lot closer to ground than satellites and are also used to provide fixed broadband connectivity as well as transmission links between mobile and core networks for backhauls.

By far the most prevalent out of these are still satellites, though the balance is shifting a little bit. For the foreseeable future, however, satellites will remain the most prevalent one due to their nature and are only becoming more robust as time goes on. [12]

2.1.2 5th Generation Mobile Network (5G)

The previous and currently still very widespread fourth-generation long-term evolution (4G LTE) technology is entirely terrestrial, relying on infrastructure that can only be built on the ground. Fifth-generation (5G) networks are, however, being heavily integrated with NTNs and show a lot of promise in that regard. The protocol itself offers reduced latency, helping to offset the main disadvantage of using NTNs, as well as generally higher speeds and is built with a much wider frequency rage in mind (though mostly higher frequencies than 4G). The nature of 5G networks requires a high count of much smaller stations – compared to 4G where large, ground towers are enough to cover a good area. This, together with a number of other unique requirements, means that the rollout of 5G is still ongoing and provides a unique opportunity to entwine it with NTNs that 4G was not able to be compatible with. [13]

5G also brings with it heavy support for IoT, allowing interfacing and connections between nearly any device imaginable. This is expected to bring a plethora of new devices into the network, increasing both the amount of endpoints as well as the attack surface. With Narrowband IoT (NB-IoT) providing more energy and cost effective connectivity to objects distributed over a very wide geographical area, devices connected to the internet can be as simple as tiny agricultural sensors and utility meters or asset trackers. The mobile nature of some of these devices also encourages the more widespread adoption of NTNs into everyday life. [14]

Another of 5G's fundamental features that sets it apart from 4G is network slicing. Network slicing allows every slice to have its own logical topology, rules, and various other properties. These slices can be solely dedicated to their purposes, allowing for the prioritization of specific targets or isolating traffic to particular endpoints, whether it be users or a type of device. Being able to custom-tailor the delivery according to the needs

and requirements of the receiver allows for a single piece of hardware to serve an unprecedented amount of groups. Naturally, these capabilities make it even more of a fit for NTNs, whose high deployment costs would benefit greatly from being able to customize the network environment to several groups at once. [15]

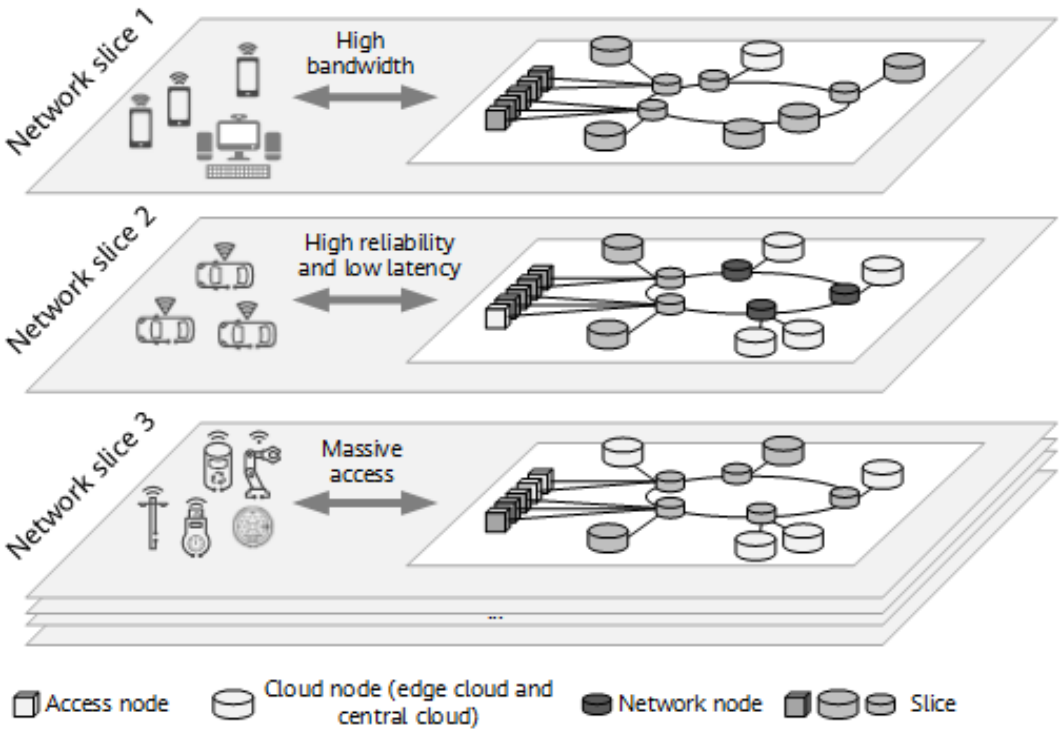

Figure 3. Example of Network Slicing [40]

The final key physical layer technology relevant to this paper is massive MIMO, referring to a base station being equipped with a very large number of antenna elements in order to improve spectral and energy efficiency. While not unique to 5G, the high frequencies rampant in 5G require massive MIMO to be more apparent than ever before, as it allows for boosting signal power to make up for the signal power drop due to path loss in high frequencies. Given its high directionality, it also reduces interference – further enabling NTNs. [16]

Table 1. Comparison of Traditional MIMO and Massive MIMO systems. [16]

	MIMO	**Massive MIMO**
Number of Antenna	<9	>15
Pilot Contamination	Low	High

	MIMO	Massive MIMO
Throughput	Low	High
Antenna Coupling	Low	High
Bit Error Rate	High	Low
Noise Resistance	Low	High
Diversity/Capacity Gain	Low	High
Energy Efficiency	Low	High
Cost	Low	High
Complexity	Low	High
Scalability	Low	High
Link Stability	Low	High
Antenna Correlation	Low	High

2.2 Vulnerabilities

With all the new technologies introduced by 5G, it also brings with itself a host of new vulnerabilities. For the purposes of this paper, only three of those will be considered, though it has to be noted that there are many, many more.

2.2.1 DOS attacks

Distributed Denial of Service attacks are one of the most common types of attacks around due to the ease of launching them, and the scale of the attacks is bigger than ever before – reaching all the way up to a recent 26 million request per second attack. [18] The war in Ukraine has also resulted in a large amount of cyberattacks from partisans of either side independently attempting to target opposing countries' infrastructure, with the easiest attack vector available to them being a simple DDoS attack. [17] However, for 5G networks, particularly in the case of ones integrated with NTNs, the most prevalent attack form is predicted to be a DOS attack as the evolution of IoT brings network capabilities to a myriad of tiny devices. This will result in an explosive growth

in the number of network connections, allowing for much more localized DOS attacks that rely on the tremendous amount of connected devices envisioned to be able to work in a 5G environment. Regardless of whether an attack intends to target the network infrastructure or a specific user, it can indirectly impact a large portion of an operator's infrastructure. [6]

2.2.2 Network slice separation

The purpose of network slices is to have users be separated into different network areas with isolated data and security protocols, which is a concept very familiar in IT through various virtualization software. In those cases, it is of paramount importance that the virtualized containers act as if there are no other such containers – being entirely separated with no movement or even hints across them. The same applies to network slices, which add a lot of complexity to a network and the current standards for implementing its security are fairly improper and not very clear. Lackluster handling of the policies and the execution of network slices could potentially allow malicious actors to gain access to data from slices they are not authorized to view or even potentially modify their operations, most notably blocking timely access for other users. [8]

2.2.3 MIMO pilot contamination

Pilot contamination is a fairly familiar kind of phenomenon in any type of wireless communication as it relies on the superposition of wireless signals, though in this paper the contamination of specifically a pilot signal is discussed. A pilot signal is a predefined reference signal that is transmitted to the receiver so that the channel it propagated over can be estimated. The contamination issue arises from two terminals transmitting simultaneously, therefore making the base station receive a superposition of the signals and make a false estimate. In the best case scenario it leads to a loss of availability for the terminal(s), though in the worst case scenario the base station might unintentionally transmit some of the beamformed downlink signal towards the interferer. [9] [19]

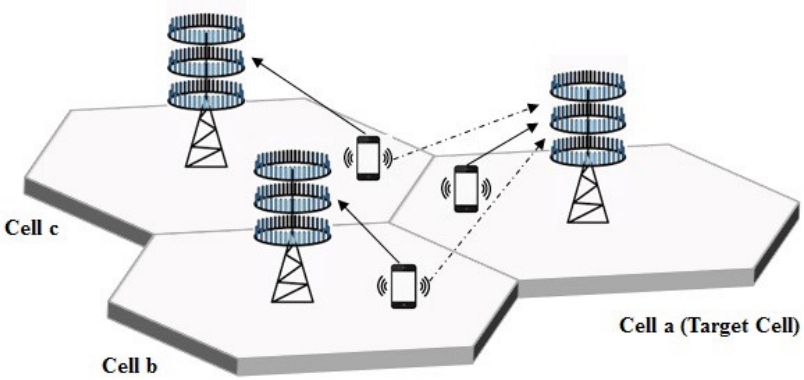

Figure 4. Example of MIMO pilot contamination (cell a contaminated)[39]

3 Methodology

The research contained in this paper is a meta-analysis both due to the scope and nature of the topic at hand, where it is not feasible to provide any sort of tangible, physical output nor is it reasonable for the scope of a bachelor's thesis to attempt to revolutionize findings in an area that is currently being thoroughly researched. Instead, this thesis aims to do a systematic review (SR) in order to identify the research papers and other information out there that is relevant to the topic at hand and deserves to be included in the paper. Because of the large involvement of multiple different types of parties such as governments, companies, volunteers, and researchers – not all sources should be scientific journals. The security of these systems is of paramount importance for the future and therefore every avenue of information must be considered – including but not limited to government write-ups, systematic information of the designers of the systems and architectures, advisory boards on the topics, as well as research papers.

After a systematic review has been performed, the most relevant and vital data is extracted from the sources and included in this paper in a condensed manner and with some supplementary analysis from the author of this paper. Should any given sources contradict each other, it will be specifically brought out with some additional elaboration and consideration given to the viewpoints of the sources on the given issue.

There are a fair share of similar papers on the general topic, however they are largely short (~5 pages), very technical papers that go over the subject matter in a manner that would not be understandable to the more general public this paper is intended for, or they are extensively long papers that either only briefly touch on 5G or NTNs or focus heavily on a single technology, often without the context of the two techologies put together. As such, there is a notable lack of work done in a homogenous manner to this paper.

4 Analysis of Solutions

As mentioned beforehand, this chapter contains the analysis of all the presented solutions from the sources selected through the systematic review process. There are three subchapters, one for each specific vulnerability/attack vector and with a subchapters to each of those targeting a specific solution.

4.1 DOS attacks

DOS attacks will be one of the most prevalent attack types on a 5G network due to the explosive amount of new devices and mostly target the **availability** of information. This is especially true for NTNs, whose expected use case lies in servicing as wide of an area as possible, especially for smaller devices which have less of a latency requirement such as meters, sensors, and cameras, with a minimal amount of hardware devices providing the service itself. The prevalence of IoT in 5G networks also means that the types of requests made can vary greatly and be fairly hard to pinpoint from genuine communications. Since NTNs will also serve a large number of critical infrastructure such as emergency communications, availability is key. Currently, a large number of solutions that target DOS attacks rely on redundancy to deal with sudden spikes in activity. 5G however brings with itself the potentiality for a much more sustained, wider attack that would be capable of depleting the network's resources, and as such the old solutions are no longer enough. This is even more so the case for NTNs due to redundancy being a fairly expensive option for such networks and therefore is not preferable to be implemented to an unnecessarily heavy degree if better options are available. With that in mind, some of the solutions are as follows. [21]

4.1.1 IoT device detection

Due to the nature of IoT devices, pinpointing malicious actors is potentially a lot easier as the continuous nature of the devices' access behavior could allow for detecting anomalous activity within the network. As such, an "overloaded" condition could be

used that denies or throttles access to the network for fresh connections while active. This could further be refined with the advent of AI to recognize peculiar network access patterns and then selectively deny access to such connections during the condition. Further research done on the topic has proven that reliable DOS attack detection through the use of AI is achievable. [6] [23] [24] [25]

In terms of cost, already trained AI as well as specifically training AI for specific scenarios has become a lot more accessible and is generally not very expensive, particularly compared to the cost of deploying a NTN. This type of approach is possible to be consistently iterated on as well, and the longer the network has been online the more capable the implementation would be for detecting anomalous spikes in usage and non-standard access patterns from devices of any kind, as it has a stronger reference point through time to which to compare atypical connections to.

However, this solution does potentially prevent genuine devices from accessing the network. This is partially mitigated by focusing solely on IoT devices and their unique behaviors due to there being no human in the loop, therefore allowing a large amount of the critical communications and data to persist. Despite that, it is not a catch-all solution and these behaviors could be spoofed by malicious actors, though doing so raises the attack complexity and the barrier for entry considerably. It is also possible for threat actors to attempt to bypass it by using devices already connected to the network and engaging in “chatty” behavior, coordinating bursts of activity with random amounts of inactivity between the transfers. This, too, could potentially be learned by the detection models and blocked.

The solution is very adaptive to several different types of DOS attack and comes with an extremely low cost – perfect for the already costly deployment of NTNs. As a software solution, it also has minimal cost scaling due to the number of devices. The complexity of adapting it is decreasing with time and is already at a somewhat low point, though at the rate of AI’s progress it is foreseeable to become even better. The developments in the field are also in some ways detrimental, forcing an arms race as AI has already made launching harder to detect attacks simpler as well, and therefore continuous R&D is required to keep up with the arms race. The solution also has the downside of potentially blocking important genuine connections, and as attacks get

more complex it is unlikely for that issue to be able to be overcome. The solution is also computationally somewhat expensive, which could prove to be a problem for NTNs.

4.1.2 Green Software-defined Satellite Network (SDSN)

One of the main factors in dealing with DDoS attacks in the context of NTNs is the energy efficiency. As NTNs are not "plugged in" like normal terrestrial systems, energy and computational efficiency in dealing with an incoming DDoS attack is key as merely overwhelming the DDoS attack prevention in a way that drains the NTNs can be considered a successful attack. Figure 5 provides an overview of a design that would mitigate the aforementioned problem.

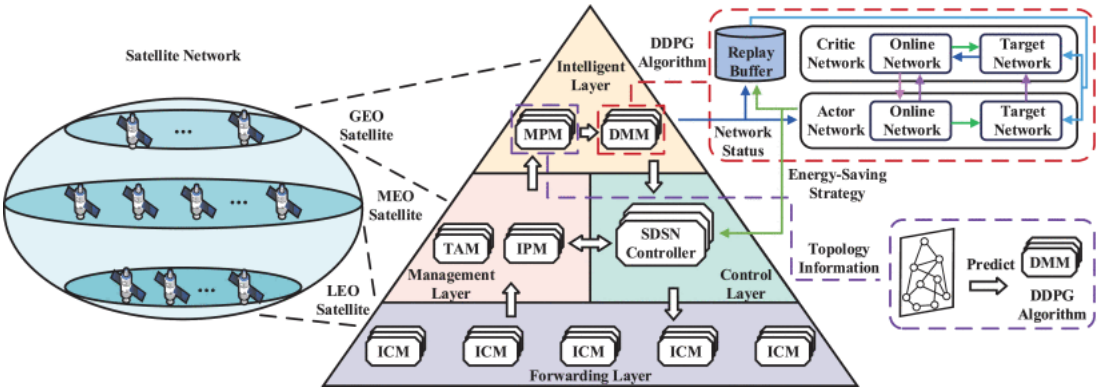

Figure 5. Example of a green SDSN framework [29]

This framework allows for a hierarchical structure that divides the network into four different layers, assigning roles based on the height of the NTN at hand, where the steps earlier on in the process are logically assigned to NTN devices lower in altitude and therefore with a lower latency. It should be noted that the forwarding layer can also consist of other NTN devices such as HAPS. In the forwarding layer, the information collection module (ICM) collects status about all the nodes in the network. Since out of all the devices in the topology only GEO satellites are stationary above a specific ground location, the topology awareness module (TAM) constructs the NTN topology at any given moment and the information processing module (IPM) aggregates all that information for use by the model prediction module (MPM) in the intelligent layer to select the proper energy-saving strategy – manifesting the DDoS mitigation model (DMM) from its choice which sends precise instructions to the SDSN controller in the

control layer that executes the instructions and sends them to every node in the forwarding layer. [26] [27] [28] [29]

This technology's by far biggest advantage is its resource and energy efficiency per involved node. As those parameters are very different for a NTN compared to a terrestrial one and are by nature limited, it is imperative to save them wherever possible. The solution presented in great depth in [29] provides a framework for mitigating energy usage by optimizing the link switching done by the TAM. It also provides a simple base mechanism for the mitigation of DDoS attacks that is simple to understand and implement, represented by Figure 6.

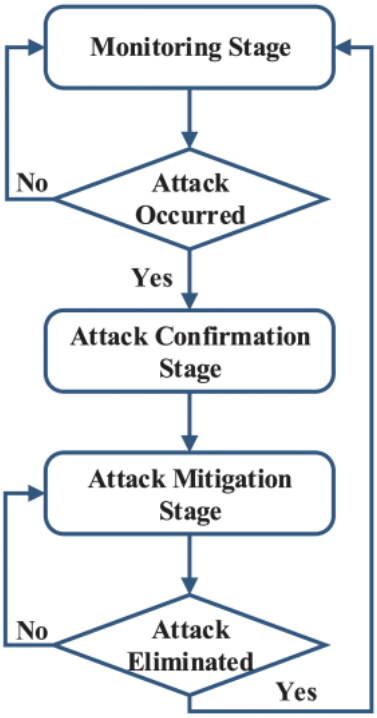

Figure 6. Green SDSN DDoS attack mitigation mechanism [29]

However, the cost and scale of implementing a system such as this is quite massive. The structure of the topology relies on a physical structure consisting of at least several nodes at varying orbital heights, which makes it nigh impossible for a small actor to utilize. Doing so without controlling the entirety of the SDSN alone requires teamwork between multiple different actors and considerably raises the complexity of the system, making it more prone to errors and mishandlings resulting from the long chain involved. As a large-scale solution, trying to use this implementation is expensive in terms of both time and funds, and is even more difficult when potentially allowing for new nodes to be added, especially from new actors. Due to the number of nodes involved in the

solution, the attack surface is very wide and while it may handle DDoS attacks of various types fairly well, it leaves it more vulnerable to other types of attacks. Should multiple actors be involved in the management of the SDSN and contributing nodes to it, the human threat actor increases and is in some part out of the control of any given individual contributor. [29]

While the system proposed also offers an implementation of a deep deterministic policy gradient (DDPG) algorithm that would be able to perform analysis based on a more continuous action space[30] that is prevalent in NTNs, the performance of the algorithm itself must strike a balance between the attributes of the algorithm (its learning and update rate) and the performance of the mitigation model as a whole, lest the endeavor be moot and bring more resource consumption than the model itself saves.

However, the green SDSN implementation can be taken in parts as well, using one's own policies and different procedures for mitigating DDoS attacks of various types – only using the general structure of the mitigation mechanism outlined in Figure 6 and/or the topology of the network described in Figure 5. One could also integrate both of the DOS strategies mentioned in this paper, using the solution developed in 4.1.1 as part of the mitigation strategies employed by the DMM.

4.2 Network slice separation

Network slicing is a fundamental feature in 5G and one that will undoubtedly be implemented in NTNs due to the cost and rigidity of launching additional hardware into the network. As it allows for separating the logical networks on top of a shared infrastructure, its security is extremely important as being able to access slices an actor is not authorized to would compromise the entire NTN and render it unreliable to use. Attacks aimed at exploiting network slicing target the **confidentiality** of the information in the NTN, though can also target the other pillars. Since not implementing network slicing in 5G is largely out of the question and so is not handling the separation issue, some solutions are outlined below. [20] [22]

4.2.1 Automatic Mapping of Cyber Security Requirements

Figure 7 (below) shows a general outline of a potential design for a network management solution that would be dynamic and automatic, as well as continuous enough to support NTN operation and be future-proof enough to be viable for implementation in such a network. The parts in gray are relevant to the model at hand. The requirements of the business applications (top-down) and the underlying technologies supporting them (bottom-up) are both collecting in a model independent of the technologies themselves and provide the software-defined networking (SDN) controlled with the required information. These are both rated in terms of the fundamental requirements (FRs) outlined in the ISO standard, making them much more machine readable. [32]

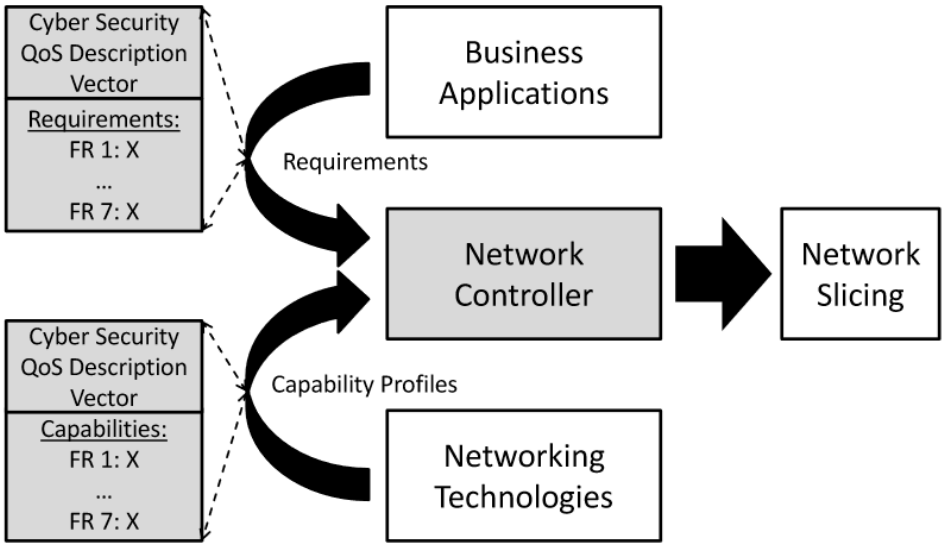

Figure 7. Potential future network management solution [32]

The model itself is fairly basic in principle and allows for a lot of adaptation based on the needs and capabilities of the actor implementing them. The cost for a simple implementation is very minimal in both computational resources and price as well as the overall maintenance that has to be performed on the system not being very high. This kind of system would allow NTN providers to very quickly adapt to the business needs of the end users and create network slices exactly tailored to the quality of service (QoS) requirements. The human input required for creating new slices is low as only the technologies respective to the FRs and their levels need to be described.

This solution provides a simple and modular way to create new network slices as well as manage them and potentially update them as well – if new network technologies come into play then the respective FRs could be updated and the controller can simply upgrade or change the implemented solutions based on the already established requirement levels of any given slice. While FRs are also a good guideline, the system could be expanded upon to use more specific criteria that the NTN operator wishes for.

However, it only serves as an automation of the security needs and helps deliver the network slices in accordance to the rough requirements of the end user group. The system itself does not provide any intrinsic security and should it be compromised in any manner the threat actor would be able to simultaneously alter the properties of every network slice in the NTN.

4.2.2 Security Trust Zones

Perhaps an evolution of the previous model, security trust zones (STZ) allow for more fine-tuned control over the network slices that get deployed in an NTN. The main property of these zones is the usage of an in-depth template that covers very specifically the particular rules put in place at any given subset inside of any given slice and the mechanisms and components deployed both into the slice and outside of it. This model allows for finer control over the small details both at deployment and during runtime. One of the more unique aspects of this kind of approach is the self-healing aspect, allowing the STZs to perform autonomously from other parts of the given network slice – relying partly on the difference between rules deployed and rules active which can dynamically change inside of a given STZ as seen in Table 2. [34]

Table 2. STZ profiling template [34]

Group	**Property**
General	STZ Level
	Privacy Level
	Integrity Level
Detection capabilities	Threats
	Rules Deployed
	Rules Active

Group	Property
	Sensors Deployed
	Sensors Active
	Events
	Alarms Triggered
Prevention Capabilities	Threats
	Rules Deployed
	Rules Active
	Sensors Deployed
	Sensors Active
	Events
	Alarms Triggered
Reaction Capabilities	Countermeasures
	Rules Deployed
	Rules Active
	Actuators Deployed
	Actuators Active
	Alarms
Self-healing capabilities	Reconfiguration Rules
	Autonomy Rules
Threat intelligence exchange	Conversion Plugins
	Normalization Plugins
	Privacy-preserving Plugins

In the case of NTNs where computational and energy resources are extremely important, having a system that allows for adapting to the situation currently ongoing inside of a slide in order to save computational resources benefits the infrastructure very heavily and allows for much better availability of resources – helping the core functions

of the NTN itself. The cost of building this kind of a system is however in ways higher than the previous described solution. While the process of customizing the template and creating all the data for a STZ or few takes considerably less time than building the entirety of an automated mapping system, the ongoing maintenance of this type of approach is significantly more costly in terms of time and will become exponentially more so as the amount of STZs increases. This type of semi-manual approach does however allow tailoring the system more specifically for the requirements of a given subset inside of a slice – which is preferable in the case of lower amounts of served groups. This is generally not the case for NTNs which tend to serve a large amount of different groups over a very wide area, only becoming more diverse with the advent of 5G.

One of the benefits of this approach – the ability to create a STZ for a specific subset inside of a network slice, or even create multiple STZs inside of a single slice, is also one of its main weaknesses. As the group in need of a special security solution shares a network slice with other groups, the threat of confidentiality being broken is potentially even heavier and special consideration has to be taken regarding that. This model could however be adapted together with the previous one and they would potentially work in harmony, whether or not the entire concept of the STZ is used alongside a more automated solution described in 4.2.1 or if only ideas from the template are borrowed.

4.3 Massive MIMO pilot contamination

Pilot contamination is the last vulnerability described in this paper. While this sort of phenomenon can occur both intentionally and non-intentionally and solutions tend to target both cases, the paper refers to it in general as an attack. This type of attack targets the **integrity** part of the data in particular, though other pillars may experience potential adversities as well. Since massive MIMO is becoming nearly mandatory in the deployment of NTNs due to the higher frequencies used in 5G, care must be taken to secure them from this type of attack. As such, some solutions are outlined below.

4.3.1 Superimposed pilots

Superimposed pilots refers to adding both the pilot and data samples of a transmission together instead of first sending the pilots and then sending the data. In this scenario, pilots and data are being continuously transmitted by adding them together. When beamforming down and estimating for the purposes of doing so, pilot contamination is almost entirely eliminated with this method. However, it brings with itself a lot of overhead which is not great for the resource efficiency required for NTNs and while it may greatly help with pilot contamination, it ends up contaminating the data instead with the pilots and creating a lot of interference. This type of method also cannot fully alleviate pilot contamination unless the frame is infinitely large. [35] [36]

Figure 8. Superimposed pilots versus orthogonal pilots [38] highlights the difference between more classical orthogonal pilots and superimposed ones.

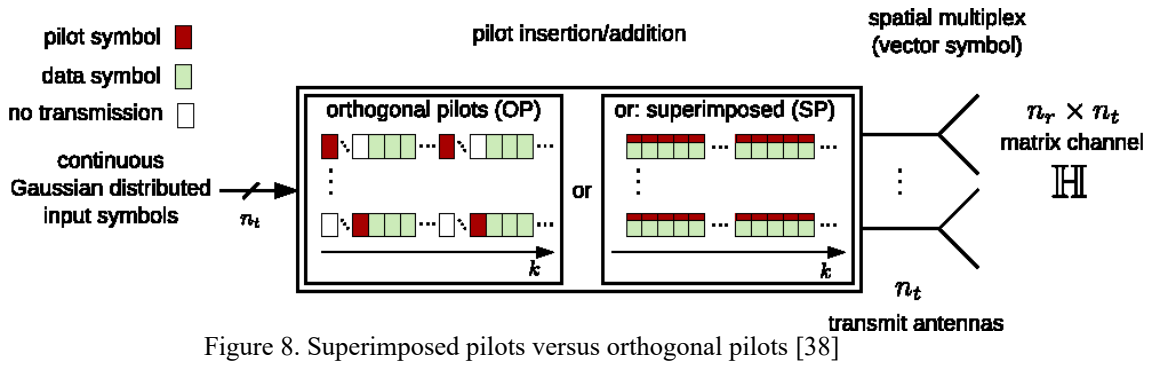

Figure 8. Superimposed pilots versus orthogonal pilots [38]

4.3.2 Channel Estimation with Spatial Correlation

This technique is still somewhat new in the world of pilot contamination and is therefore in the process of being refined, however it is a big step forward in solving the problem of pilot contamination and could entirely eliminate it if successfully implemented. The principle is to utilize partially blind estimates in order to separate the subspace of desired user equipment channels from the subspace of interfering channels. Despite theoretically being able to fully remove pilot contamination if the number of antennas and the size of the channel coherence block go jointly to infinity, that is not the case in reality. To this day it is one of the best solutions possible for the pilot contamination problem, as more antennae can be added in order to support a larger amount of users – though the payoff is logarithmic by nature and will eventually become less worthwhile and by then a new solution will hopefully be devised. This

solution is superior to the aforementioned one in massive MIMOs in every regard and as such there is no cost analysis to be made. [37]

5 Future Research

Because of the inherent nature of a bachelor's thesis, the research and scope of this paper had to be considerably toned down – though a full analysis of every present method is nigh impossible in scope regardless. Nearly all of the solutions and problems mentioned in this paper are enough for a research paper of their own if done in the context of NTNs, or some even in their own right.

In particular the research scene for massive MIMO pilot contamination is severely lacking in contributors with the same names popping up in a majority of the researches on the topic – let alone taking the context of NTNs into account, and the possibilities provided by channel estimation with spacial correlation are still highly experimental with the authors calling for more contributions in their paper.

This paper itself could be expanded with many more vulnerabilities and many solutions per each vulnerability as well, though that was regarded as out of the scope of this thesis. Regardless, there is a void in the field of 5G and NTN integration that the author fears will not be filled in time, seeing as talks of 6G are already underway and research starts to drift away to focus on that instead.

Increasing the count of either the vulnerabilities discussed or focusing the research on a single vulnerability and its solutions can also provide necessary insight into areas and help compare the information available in a unique manner not possible in thesis discussing more general concepts or states of mentioned issues.

6 Summary

The aim of this paper was to condense some information available on the topics, analyzing them in a particularly NTN focused manner which is something the field is sorely lacking. In particular the author chose three different vulnerabilities that each stand for one of the main pillars of cyber security: confidentiality, integrity, and availability, and decided to analyze existing research in the areas of the chosen vulnerabilities. Two solutions were chosen for each vulnerability in order to highlight different viewpoints and approaches to a problem as well as highlight that often times mixing and taking the best and most fitting parts of various different solutions in accordance to the needs of the developed system is the best choice. There is rarely a best solution available and even if the entirety of a given solution may not fit – parts of it could still be adapted and used along with own ideas or other solutions, combining them to create a much more secure and adaptive system.

However, the solutions for the pilot contamination problem were chosen to specifically point out that sometimes, even if solutions sound reasonable – there might still be a clearly, objectively better solution out there as well. It served to highlight this somewhat rare phenomenon which is especially prevalent in the field of mathematics and physics. Were it not for the precondition of massive MIMO (which is a favourable system for NTNs and therefore a perfect fit), alternative solutions could have been better with a lower amount of antennae.

Throughout the research it was also found that the majority of information existing on the topic is somewhat unorganized and presented in a way that is too technical for executives to understand. This paper serves additionally provide an example of potentially presenting such information in a manner that is more understandable and to also give an example of realistic, effective comparison of solutions where the solution is not always blindly following an existing one but instead careful consideration.

References

[1] Rodriguez-Donaire, S., Sureda, M., Garcia-Almiñana, D., Sierra, E., S. Perez, J., C.E. Roberts, P., … Heißerer, B. (2020). Earth Observation Technologies: Low-End-Market Disruptive Innovation. IntechOpen. doi: 10.5772/intechopen.90923

[2] European Commission – Directorate-General for Communication Networks, Content and Technology (CONNECT), “Transformation of the connectivity sector in the EU ”, February 2023. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_985

[3] Viasat, Inc., “KA-SAT Network cyber attack overview”, March 2022. [Online]. Available: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

[4] Holmes, M., “The Growing Risk of a Major Satellite Cyber Attack”, 2022. [Online]. Available: https://interactive.satellitetoday.com/the-growing-risk-of-a-major-satellite-cyber-attack/

[5] Next Generation Mobile Networks, “NGMN 5G White Paper”, February 2015. [Online]. Available: https://ngmn.org/wp-content/uploads/NGMN_5G_White_Paper_V1_0.pdf

[6] Next Generation Mobile Networks, “5G security recommendations Package #1”, May 2016. [Online]. Available: https://ngmn.org/wp-content/uploads/Publications/2016/160506_NGMN_5G_Security_Package_1_v1_0.pdf

[7] F. Z. Yousaf, M. Bredel, S. Schaller and F. Schneider, "NFV and SDN—Key Technology Enablers for 5G Networks," in IEEE Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2468-2478, Nov. 2017, doi: 10.1109/JSAC.2017.2760418.

[8] National Security Agency & The Cybersecurity and Infrastructure Security Agency, “ESF Potential Threats to 5G Network Slicing”, December 2022. [Online]. Available: https://media.defense.gov/2022/Dec/13/2003132073/-1/-1/0/POTENTIAL%20THREATS%20TO%205G%20NETWORK%20SLICING_508C_FINAL.PDF

[9] Gülgün, Z. (2021). Physical Layer Security Issues in Massive MIMO and GNSS (Licentiate dissertation, Linköping University Electronic Press). https://doi.org/10.3384/lic.diva-172558

[10] NASA, “Explorer and Early Satellites”, January 2018. [Online]. Available: https://www.nasa.gov/mission_pages/explorer/index.html

[11] Union of Concerned Scientists, “UCS Satellite Database”, May 2022. [Online]. Available: https://www.ucsusa.org/resources/satellite-database

[12] Communications, Space & Technology Commission, “Non-Terrestrial Networks Program”, April 2023. [Online]. Available: https://www.cst.gov.sa/en/ntn/Pages/default.aspx

[13] 3GPP, “System architecture for the 5G System” (TS 23.501), April 2023. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144

[14] D. Flore, 3GPP Standards for the Internet-of-Things, February 2016, [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1766-iotprogress

[15] 3GPP, TS 28.530, December 2019. [Online]. Available: https://www.3gpp.org/ftp/tsg_sa/WG5_TM/TSGS5_128/SA_86/28530-f30.doc

[16] Chataut R, Akl R. Massive MIMO Systems for 5G and beyond Networks—Overview, Recent Trends, Challenges, and Future Research Direction. Sensors. 2020; 20(10):2753. https://doi.org/10.3390/s20102753

[17] Cloudflare, “DdoS attack trends for 2022 Q2”, June 2022. [Online]. Available: https://blog.cloudflare.com/ddos-attack-trends-for-2022-q2/

[18] Cloudflare, “Cloudflare mitigates 26 million request per second DdoS attack”, June 2022. [Online]. Available: https://blog.cloudflare.com/26m-rps-ddos/

[19] Wu, Y., Liu, T., Cao, M. et al. Pilot contamination reduction in massive MIMO systems based on pilot scheduling. J Wireless Com Network 2018, 21 (2018). https://doi.org/10.1186/s13638-018-1029-1

[20] Wang, M., Zhu, T., Zhang, T., Zhang, J., Yu, S., & Zhou, W. (2020). Security and privacy in 6G networks: New areas and new challenges. Digital Communications and Networks, 6(3), 281–291. https://doi.org/10.1016/j.dcan.2020.07.003

[21] X. Lin, S. Rommer, S. Euler, E. A. Yavuz and R. S. Karlsson, "5G from Space: An Overview of 3GPP Non-Terrestrial Networks," in IEEE Communications Standards Magazine, vol. 5, no. 4, pp. 147-153, December 2021, doi: 10.1109/MCOMSTD.011.2100038.

[22] Pietro Tedeschi, Savio Sciancalepore, and Roberto Di Pietro. 2022. Satellite-based communications security: A survey of threats, solutions, and research challenges. Comput. Netw. 216, C (Oct 2022). https://doi.org/10.1016/j.comnet.2022.109246

[23] Cyber Physical Systems Public Working Group, “Framework for Cyber-Physical Systems Volume 1”, March 2017. [Online]. Available at: https://doi.org/10.6028/NIST.SP.1500-201

[24] Veranyurt, O., Usage of Artificial Intelligence in DOS/DDOS Attack Detection, June 2019.

[25] Martin Zadnik and Elena Carasec. 2022. AI infers DoS mitigation rules. J. Intell. Inf. Syst. 60, 2 (Apr 2023), 305–324. https://doi.org/10.1007/s10844-022-00728-2

[26] M. Onen and R. Molva, "Denial of service prevention in satellite networks," 2004 IEEE International Conference on Communications (IEEE Cat. No.04CH37577), Paris, France, 2004, pp. 4387-4391 Vol.7, doi: 10.1109/ICC.2004.1313376.

[27] Abdelsalam, N., Al+Kuwari, S. & Erbad, A., Physical Layer Security in Satellite Communication: State-of-the-art and Open Problems, Jan 2023.

[28] Zhang, Y.; Wang, Y.; Hu, Y.; Lin, Z.; Zhai, Y.; Wang, L.; Zhao, Q.; Wen, K.; Kang, L. Security Performance Analysis of LEO Satellite Constellation Networks under DDoS Attack. Sensors 2022, 22, 7286. https://doi.org/10.3390/s22197286

[29] Z. Tu, H. Zhou, K. Li, M. Li and A. Tian, "An Energy-Efficient Topology Design and DDoS Attacks Mitigation for Green Software-Defined Satellite Network," in IEEE Access, vol. 8, pp. 211434-211450, 2020, doi: 10.1109/ACCESS.2020.3039975.

[30] W. Shi, D. Gao, H. Zhou, Q. Xu and C. H. Foh, "Traffic Aware Inter-Layer Contact Selection for Multi-Layer Satellite Terrestrial Network," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-7, doi: 10.1109/GLOCOM.2017.8254661.

[31] Cunha, VA, Silva, E, Carvalho, MB, et al. Network slicing security: Challenges and directions. Internet Technology Letters. 2019; 2:e125. https://doi.org/10.1002/itl2.125

[32] M. Ehrlich, L. Wisniewski, H. Trsek, D. Mahrenholz and J. Jasperneite, "Automatic mapping of cyber security requirements to support network slicing in software-defined networks," 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Limassol, Cyprus, 2017, pp. 1-4, doi: 10.1109/ETFA.2017.8247728.

[33] Kotulski, Z., Nowak, T., Sepczuk, M. et al. Towards constructive approach to end-to-end slice isolation in 5G networks. EURASIP J. on Info. Security 2018, 2 (2018). https://doi.org/10.1186/s13635-018-0072-0

[34] D. Schinianakis, R. Trapero, D. S. Michalopoulos and B. G. -N. Crespo, "Security Considerations in 5G Networks: A Slice-Aware Trust Zone Approach," 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 2019, pp. 1-8, doi: 10.1109/WCNC.2019.8885658.

[35] K. Upadhya, S. A. Vorobyov and M. Vehkapera, "Superimposed Pilots Are Superior for Mitigating Pilot Contamination in Massive MIMO," in IEEE Transactions on Signal Processing, vol. 65, no. 11, pp. 2917-2932, 1 June1, 2017, doi: 10.1109/TSP.2017.2675859.

[36] D. Verenzuela, E. Björnson and L. Sanguinetti, "Spectral and Energy Efficiency of Superimposed Pilots in Uplink Massive MIMO," in IEEE Transactions on Wireless Communications, vol. 17, no. 11, pp. 7099-7115, Nov. 2018, doi: 10.1109/TWC.2018.2860939.

[37] E. Björnson, J. Hoydis and L. Sanguinetti, "Massive MIMO Has Unlimited Capacity," in IEEE Transactions on Wireless Communications, vol. 17, no. 1, pp. 574-590, Jan. 2018, doi: 10.1109/TWC.2017.2768423.

[38] A. T. Asyhari and S. ten Brink, "Orthogonal or Superimposed Pilots? A Rate-Efficient Channel Estimation Strategy for Stationary MIMO Fading Channels," in IEEE Transactions on Wireless Communications, vol. 16, no. 5, pp. 2776-2789, May 2017, doi: 10.1109/TWC.2017.2665467.

[39] Al-hubaishi AS, Noordin NK, Sali A, Subramaniam S, Mohammed Mansoor A. An Efficient Pilot Assignment Scheme for Addressing Pilot Contamination in Multicell Massive MIMO Systems. Electronics. 2019; 8(4):372. https://doi.org/10.3390/electronics8040372

[40] What is Network Slicing? Available at: https://info.support.huawei.com/info-finder/encyclopedia/en/Network+Slicing.html [accessed 4 April, 2023]

[41] Jukka-Peeka Nuutinen, Non-Terrestrial Network Realities Call for New 5G Testing Approaches, Available at: https://www.spirent.com/blogs/non-terrestrial-network-realities-call-for-new-5g-testing-approaches [accessed 3 April, 2023]

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Gustav Gretškov

1 Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis „An Analysis of the Security Shortcomings of 5G Architecture in Non-Terrestrial Networks", supervised by Aleksei Talisainen

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2 I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3 I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

01.04.2023

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.