Uplink security against airborne adversaries in non-geostationary satellite communications

Markus Säynevirta

School of Electrical Engineering

Thesis submitted for examination for the degree of Master of Science in Technology.
Espoo 31.12.2023

Supervisor

Asst. Prof. Jaan Praks

Advisor

M. Sc. (Tech) Tapio Savunen

Aalto University
School of Electrical
Engineering

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

Author Markus Säynevirta

Title Uplink security against airborne adversaries in non-geostationary satellite communications

Degree programme Master's Programme in Automation and Electrical Engineering

Major Electronic and Digital Systems **Code of major** ELEC3060

Supervisor Asst. Prof. Jaan Praks

Advisor M. Sc. (Tech) Tapio Savunen

Date 31.12.2023 **Number of pages** 52+2 **Language** English

Abstract

Your abstract in English. Keep the abstract short. The abstract explains your research topic, the methods you have used, and the results you obtained.

The abstract text of this thesis is written on the readable abstract page as well as into the pdf file's metadata via the \thesisabstract macro (see above). Write here the text that goes onto the readable abstract page. You can have special characters, linebreaks, and paragraphs here. Otherwise, this abstract text must be identical to the metadata abstract text.

If your abstract does not contain special characters and it does not require paragraphs, you may take advantage of the abstracttext macro (see the comment below).

Keywords For keywords choose, concepts that are, central to your, thesis

Aalto University
School of Electrical
Engineering

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

Tekijä Markus Säynevirta

Työn nimi Uplink-liikenteen suojaus vihollisen ilma-aluksia vastaan ei-geostationaarisessa satelliittiviestinnässä

Koulutusohjelma Elektroniikka ja sähkötekniikka

Pääaine Elektroniset ja digitaaliset järjestelmät **Pääaineen koodi** ELEC3060

Työn valvoja Apul. prof. Jaan Praks

Työn ohjaaja DI Tapio Savunen

Päivämäärä 31.12.2023 **Sivumäärä** 52+2 **Kieli** Englanti

Tiivistelmä

Tiivistelmässä on lyhyt selvitys kirjoituksen tärkeimmästä sisällöstä: mitä ja miten on tutkittu, sekä mitä tuloksia on saatu.

Avainsanat Vastus, resistanssi, lämpötila

Preface

I want to thank Professor Pirjo Professori and my instructor Dr Alan Advisor for their good and poor guidance.

Espoo, 31.7.2023

Markus Säynevirta

Contents

Symbols and abbreviations

Symbols

$\mathbf{B}$	magnetic flux density
c	speed of light in vacuum $\approx 3 \times 10^8$ [m/s]
ω_{D}	Debye frequency
ω_{latt}	average phonon frequency of lattice
$\uparrow$	electron spin direction up
$\downarrow$	electron spin direction down

Abbreviations

COMINT	communications intelligence
ELINT	electronic intelligence
EO	earth observation
ES	electromagnetic support
FSS	fixed satellite service
GNSS	global navigation satllite system
ISR	intelligence, surveillance, and reconnaissance
MSS	mobile satellite service
NTN	non-terrestrial network
satcom	satellite communication
SIGINT	signals intelligence

1 Introduction

Over the past five decades, satellite systems have emerged as indispensable enablers of our modern way of life within an increasingly technology-driven human society. Innovation in fields such as Global Navigation Satellite Systems (GNSS) [1], Earth Observation (EO) [2, 3], and Satellite Communication (satcom) [4] has brought us ubiquitous connectivity in every corner of this world, while unlocking previously unimaginable capabilities in position, navigation, and timing (PNT), as well as intelligence, surveillance, and reconnaissance (ISR). Recently, the satellite communications industry has entered into an era of rapid change. Since the early 2010s, the most prominent new trend has been the large megaconstellations of hundreds to thousands of satellites in Low Earth Orbit (LEO). These have been enabled by the falling cost of space launches and mass-production of satellite hardware based on Commercial Off-The-Shelf (COTS) technology.

Aside from commercial markets, governmental organisations such as civilian public safety authorities and defense ministries have expressed great interest in emerging commercial satellite communication solutions. In terms of user segments, governmental organisations tend to pay greater attention to the security and resilience aspects of the communications solutions they utilise, which has in turn raised questions regarding the conformity of these systems.

Protecting these commercial satellite systems against a growing number of increasingly cyber-capable adversaries has become a prerequisite for adopting new satellite systems by governmental agencies. Here, robust understanding of the evolving threat landscape is a key starting point for design of effective cybersecurity measures. Recently, LEO broadband systems have been increasingly used by commercial and government actors for satellite system security.

Despite their decades-long development history, current satellite systems still lack widely accepted cybersecurity standards [5]. Varying technical solutions and their proprietary nature has raised a set of potential vulnerabilities. Moreover, the wide-area broadcast nature of satellite transmissions renders them vulnerable to adversarial groups from abroad or even across an entire continent. This was demonstrated in [6] where the feasibility of eavesdropping downlink satellite traffic was proven practically using widely available and relatively inexpensive satellite television equipment. Within the field of wireless communication, one key driver for this development have been the proliferation of inexpensive signals processing equipment, such as open source and open hardware Software-Defined Radios (SDR). These devices have enabled interaction with satellite systems by not only nation states but also even individual enthusiast-level actors. Moreover, the vulnerabilities in satellite systems are not limited to only the air interface of these commercial systems. Another third-party vulnerability assessment [7] uncovered serious design flaws in the implementation of satellite user terminal firmware, such as backdoors, hardcoded credentials, weak encryption algorithms as well as undocumented and insecure protocols.

Recent adversarial actions against satellite systems and their supporting infrastructure have raised questions concerning the vulnerability of these systems to a

range of potential attack vectors, including cyberattacks, as well as the physical destruction of individual satellites or their supporting ground infrastructure. Recent examples include the cyberattack against the KA-SAT satellite network in February 2022 [8] or the cable cut in one of the optical cables connecting the the SvalSat ground station to mainland Norway [9]. Similarly, intrusive acts such as the Chinese high-altitude balloons flying through North American airspace in early 2023 have highlighted the threat of aerial signals intelligence platforms [10].

One way to understand the reason for these vulnerabilities is through the paradigm of "security through obscurity", a practice with a long-running history in the commercial satellite industry that relies on hiding the structure and the interfaces of the system from the public [5]. The validity of this approach has long been debated within research and industry circles [11], with the recent consensus being that security of a system should never rely exclusively on obscurity [12, 13].

Although much work has focused on long operational geostationary broadband and non-geostationary narrowband systems, as well as more long term 5G and 6G non-terrestrial networks (NTN), little attention has been directed towards the security of emerging LEO broadband systems. Moreover, most of the research on satellite system protection has examined downlink communication between the satellite and different earth stations [14]. Furthermore, more capital-intensive space or airborne platforms have received relatively little attention, with a greater emphasis being placed on the study of ground-based adversaries. Considering this prior history and recent rapid growth, it is important to better understand the security aspects of this rapidly evolving technology.

This thesis seeks to assess whether the presence of airborne eavesdroppers poses a risk to the uplink communications of emerging NGSO VSAT networks. To achieve this goal, quantitative analysis is used by developing a threat model focusing on a Walker-type LEO megaconstellation, fixed Very Small Aperture Terminals (VSAT) and airborne eavesdroppers. The resilience of LEO broadband systems will be explored using geometric and kinematic analysis, as well as link budgets based on typical hardware configurations. The developed analytical model will be evaluated numerically by comparing its results against the requirements set by both public safety and defence user groups.

The thesis is structured as follows. Chapter 2 describes the key characteristics of LEO megaconstellations, the different aerial platforms used for eavesdropping, and signals intelligence. Chapter 3 develops a threat model comprising passive and active eavesdropping, jamming, as well as signal geolocation. Chapter 4 examines the scenarios of the model in relation to the requirements set by relevant critical communications user groups. Chapter 5 discusses the results and compares these against the end-user requirements. Chapter 6 summarizes this work by discussing the security performance of LEO broadband systems and suggesting directions for future work.

2 Background

2.1 NGSO megaconstellations

2.1.1 History and recent developments

During the last five years the satellite communications industry has entered into an era of change. The most prominent new trend is the large megaconstellations with hundreds to thousands of satellites in low earth orbit (LEO). These systems have been enabled by the falling costs in space launches and the mass-production of satellite hardware based on COTS technology [15].

GEO satellites provided most of satellite internet capacity in throughput-terms until 2020 when the emerging NGSO megaconstellations started gaining significant share in the satellite internet market. Combined, SpaceX Starlink, EutelSat OneWeb, Amazon Kuiper, Telesat Lightspeed and SES O3b mPOWER have are estimated to bring roughly USD 70 billion of capital investment into the space during the deployment of their generation 1 and 2 constellations. Everything has not though been smooth sailing. Megaconstellations are a very capex heavy industry and broader economic pressures have lead to significant delays for the companies operating in the space. For example, OneWeb went through a bankruptcy restructuring following the Covid-19 pandemic, while SES's O3b mPOWER faced significant delays from the same cause. Similarly, Canadian Telesat and its Lightspeed constellation have been hit with supply chain and financing related challenges, delaying the project and leading to descoping of some of the originally planned satellite fleet. In addition to the more aforementioned more mature players currently or soon deploying their constellation, multiple actors from around the world have expressed interest in similar projects. These include everything from smaller startups like Lynk and AST SpaceMobile, developing direct-to-smartphone satellite connecitivity, to large national and multinational projects like the EU's IRIS2 program and the Chinese Guo Wang megaconstellations [16].

In terms of maturity, SpaceX, OneWeb and SES O3b mPOWER are the farthest into the deployment with full global connecitivity available as of December 2023. Amazon Kuiper and Telesat are still being developed, with service start expected for 2026 and 2027 respectively [16]. Technologically, all five constellations are characterised by their employment of dedicated and vendor-specific technologies in their implementation with all five currently operating or planning to operate on dedicated Ku and Ka-band frequencies. Additionally, their user equipment is vendor-specific in nature, be they more traditional parabolic or modern flat-panel phased array technology-based very small aperture terminals (VSAT). On the other hand, startups like Lynk and AST SpaceMobile are planning to deliver broadband service from orbit directly to unmodified 3GPP standardised 5G handsets. Support for the implementation of 5G NTN standards defined by the 3GPP to the maximum extent possible but following a gradual implementation approach is also a key requirement in the EU's IRIS^2 programme. All in all, 3GPP NTN services are still less technologically mature and have been demonstrated in practice to a very limited extent. Thus, services based on the standard are likely still to require significant R&D expenditure

before becoming a viable option. Standardised services have the greatest potential in mid to long-term timescales, while proprietary solutions are likely to dominate in the interim [17–19].

Appendix A has a table with a non-exhaustive sample of recent LEO megaconstellation projects and their key design parameters. One interesting takeaway from the metrics is the sum of the theoretical throughputs of the systems with the figure landing into a range of hundreds of terabits-per-second (Tbps). As a reference, global internet bandwidth was estimated at 1.2 petabytes-per-second globally in 2023, an order of magnitude difference when compared to the first generation NGSO systems [20]. Thus, satellite internet services are unlikely to complete replace terrestrial solutions but will act likely as a complimentary coverage and capacity solution for both commercial and government user segments.

2.1.2 Key technical characteristics

The design of a complete satellite system is a complex, multi-objective and multimodal optimisation problem due to the inherently varying conditions and constraints in the three segments. Practically speaking, this requires tackling the overall optimisation problem segment-by-segment while taking into account the requirements of the target application. In , the main elements of a LEO satellite system were characterised into distinct space, ground and user segments, which are visualised in figure **??** [21].

Space segment comprises the satellite constellation flying in orbit. Constellation optimization is typically the primary design problem in LEO-based satellite networks as the parameters, such as orbital altitude, density of satellites, the number and inclination of orbital planes and the phasing between them, affect directly the feasibility of user applications.

Ground segment optimisation tends to be more straightforward . Ground station (GS) planning involves placing a number of stations in appropriate locations around the globe. Metrics for evaluation range from the achieved sky coverage and system throughput and link capacity to the overall deployment and maintenance costs of the GS network [21].

When considering optimisation, the user segment is the most case-specific of the three. End user applications range from communication to sensing and navigation with their optimisation criteria often contradicting each other. Here, [21] raises a good example with bandwidth and carrier frequency, where higher numbers are generally desired for example in high-throughput communication applications while the opposite applies to achieving suitable link budgets for example in navigation satellite systems or when users are situated in challenging urban terrain or indoors.

The LEO altitude leads to significantly lower latency and the large number of satellites allows for relatively high overall data throughput when compared with the earlier satellite systems but still significantly lower when compared to terrestrial systems. While NGSO constellations are nothing new, the emerging operators are promising to offer magnitudes better broadband service when compared to the earlier services offered by e.g. SES O3b and Iridium while providing the services also at a

price point that is competitive with other forms of connectivity [x].

The services are built around vendor-specific user terminals working as WiFi routers that relay the communications on dedicated Ka and Ku-band frequencies to the satellite constellation.

2.1.3 OneWeb system architecture

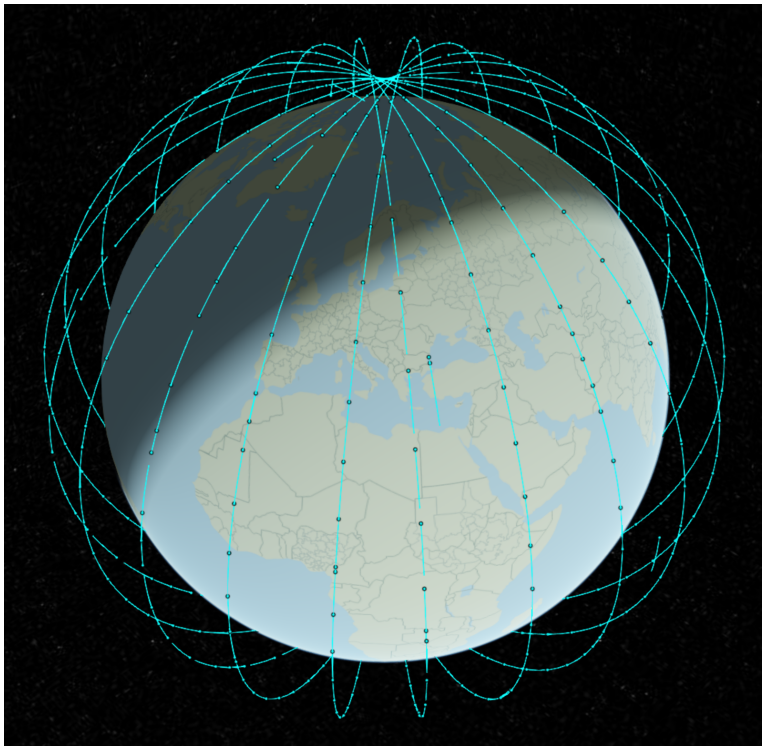

Figure 1: Simulation of the OneWeb system based on Celestrack TLE data from 11 December 2023.

The space segment of the OneWeb system comprises a megaconstellation of 648 LEO satellites distributed into 12 polar orbital planes of 49 evenly spaced satellites, as well as a number of in-orbit spares. Operational satellites fly in an inclined polar orbit with an altitude of 1200 km. Each satellite transmits and receives user terminal (UT) traffic via its 16 fixed Ku-band beams, each of which covers a geographic area with dimensions of 1600 km in longitude and 65 km in latitude. Gateway traffic is forwarded to the satellite network portals (SNP) via two identical steerable Ka-band spot beams with a significantly more focused circular coverage pattern [22, 23].

Earth Stations of the OneWeb system can be broadly divided into three categories: tracking, telemetry and control (TT&C) sites, gateways and user terminals (UTs). In the following, we will focus on the two latter ones, as they are integral to describing the end-to-end configuration of the OneWeb network [23].

Going deeper into the gateway-side architecture, the infrastructure can be further split into three components, which are network data centres (NDC), points-of-presence (PoP) and satellite network portals (SNP). NDCs host the authentication,

authorization, policy and UT databases and are deployed in key global locations. PoPs connect the OneWeb network to the Internet and are deployed at key Internet peering points. Finally, SNPs maintain the connectivity to the LEO space segment composed of the OneWeb satellite constellation. They are situated in remote locations around the globe with room for large antenna arrays of 7 to 30 full motion antennas (on average 16) equipped with a 3.5 m Ka-band dish [22].

On the user terminal side, a similar architectural breakdown can be made – the terminal consists of a satellite antenna, receiver and a customer network exchange (CNX) router. The latter connects the terminal to the end-user devices such as laptops or smartphones [22]. RF transmissions received by the satellite antenna are demodulated and converted to a digital data stream by the receiver hardware of the terminal.

As OneWeb is a LEO satellite system, UTs need to track the movements of the orbiting satellites in real-time and handover between them as they move in and out of view in order to maintain constant connectivity. This can be achieved either with traditional steerable dish or more modern phased array antenna designs. With the prior, two apertures may need to be employed for uninterrupted connectivity, as retrace speed of a single aperture is the inherent limiting factor for hand-over time between satellites. On the other hand, phased array antennas require only a single aperture as their electronic switching can be considered almost instantaneous [23].

Continuing with the distinguishing qualities of the OneWeb system, maybe the most significant is the nature of its air interface coverage pattern, also known as the cell layout. In the OneWeb satellite RAN, the cells are inherently varying and mobile, while on the contrary they are practically geographically static and pre-defined in a terrestrial network of fixed eNBs. Consequently, the movement of the UTs (for example equipment mounted on an aircraft or a high-speed train) is relatively slow when compared to the relative velocities of the satellites in orbit. This means that UT handovers happen mostly due to the orbital movement of the satellites rather than the movement of the UT relative to the surface of the earth, which is the dominating cause of UE handovers in terrestrial systems [24].

In addition to their moving nature, satellite cells are significantly larger in their coverage area when compared to their terrestrial counterparts. This has multiple consequences for [24]

In satellite systems, the link from gateway to UT via satellite is referred to as the forward link while the direction from UT to gateway is referred to as the return link. It is worth noting that both up- and downlink communications happen simultaneously in both forward and return links. For example in the return direction, a UT uplinks to and the gateway downlinks from the satellite [25]. Despite their similarities, capacity of a forward and a return link is not necessarily symmetrical. In OneWeb's case, forward link is roughly five times the capacity of the return link [15, 23].

OneWeb satellite system makes use of a bent pipe architecture for both its forward and return links. In the forward direction, each Ku-band user terminal downlink maps onto a predetermined Ka-band gateway uplink and vice-versa in the return direction. [15, 23]

Different transmission schemes are employed depending on the link direction. In

the forward direction, transmissions utilise time-division multiplexing on a single 250 MHz wideband carrier. Each user terminal receives the carrier and demodulates it, extracting relevant payload information based on the headers. [23]

a modified LTE waveform capable of adaptive modulation and coding [26]

In the return direction, transmissions utilise a single-carrier time and frequency division multiple access (SC-TDMA/FDMA) scheme. Return direction user terminal to satellite links transmit data in time bursts on a relatively narrow carrier that varies between 1.25 MHz and 20 MHz in bandwidth. Multiple user terminals are able to access a single uplink carrier based on time slots allocated by the network control centre. Terminals are also able to access multiple uplink carriers based on the FDMA channel arrangement of the satellite in question. [23]

Generally speaking, Ka-band gateway-to-satellite links are asymmetric in nature. In terms of their channel configuration, the links employ 16 up and downlink channels, bandwidth of individual channels being 155 MHz in the uplink and 250 MHz in the downlink direction. The links alternate between right and left-hand polarised (RHCP / LHCP) signals. [15]

Similar to the gateway links, the Ku-band satellite-to-user terminal links are asymmetric in nature, but at the same time they are more limited in terms of the available bandwidth. The four uplink channels occupy 125 MHz of bandwidth while there are eight 250 MHz downlink channels. Unlike the gateway links, the polarisation scheme of the signals is fixed based on the link direction, where uplink utilises RHCP and downlink LHCP. [15]

2.1.4 Starlink system architecture

SpaceX's Starlink constellation is a combination of an inclined Walker Delta and a polar Walker Star configuration. The system consists of 4,408 satellites divided into five orbital shells at altitudes ranging between 540 and 570 km. Inclination-wise, a large majority of the fleet is situated in 70 to 72 degree orbits covering the higher populated latitudes, while a reduced set in 97.6 degree orbits covering the remaining polar regions. Table 1 presents the distribution of the satellites to the orbital shells and planes in more detail [27, 28].

Table 1: Orbital shells and planes of the Starlink constellation [27].

Altitude (km)	Inclination (deg)	Planes	Satellites per plane	Total satellites
540	53.2	72	22	1584
550	53.0	72	22	1584
560	97.6	6	58	348
560	97.6	4	43	172
570	70.0	36	20	720

Starlink satellites communicate with UTs through Ku-band links. From the space segment, traffic is either relayed to other satellites via optical inter-satellite links

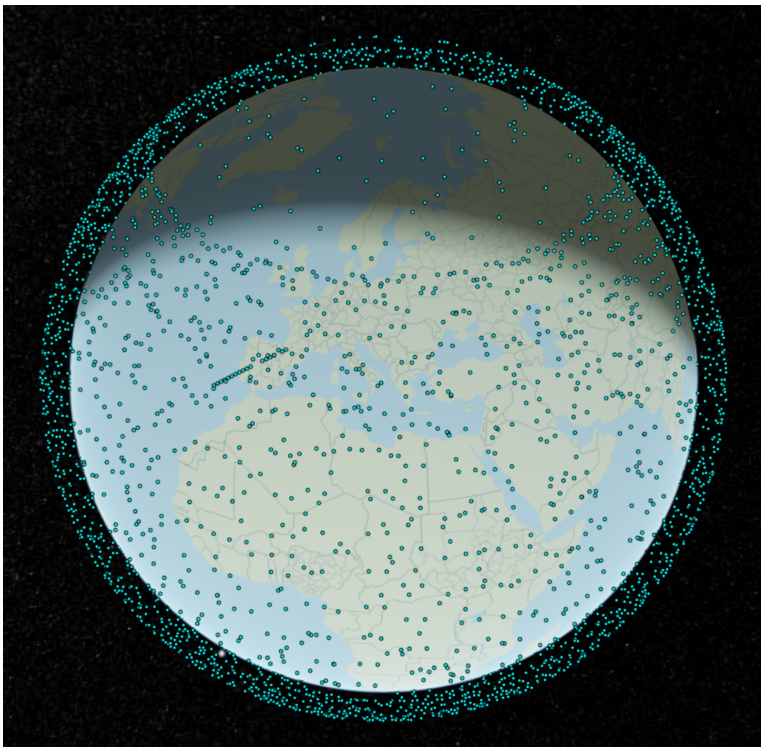

Figure 2: Simulation of the Starlink constellation based on Celestrack TLE data from 11 December 2023.

2	123

Figure 3: Frequency plan.

(ISL) or to gateways on higher frequency Ka-band links. Satellites have four phased array antennas, three of which function as downlink and one as uplink. All four arrays are // capable of projecting eight // independently shapeable and steerable spot beams, resulting in a 3-to-1 downlink-to-uplink ratio. Figure X presents Starlink and OneWeb frequency plans in relation to each other [29].

Beam radiation pattern is dependent mainly on the steering angle of the beam with angles farther from boresight making the beam footprint more elliptical. Starlink 3 dB beam footprints vary between x and x kilometers in their major axis. Minor axis varies less with values ranging between x and x kilometers depending on the beam steering angle. Overall beamwidth is controlled by selectively switching on additional array elements as the steering angle rises. Minimum elevation angle of the SpaceX system is 25 degrees [27, 29].

Ground segment 1.5 m Ka-band antennas

Starlink dish variants. Common feature ESA technology. Some flat panel while others use steering. Size varies between x and x m.

Starlink's cell pattern is based on Uber's H3 hexagonal cell system. Each spot beam covers roughly 1 size 5 hex cell at nadir. It is worth noting that the beam becomes more elliptical at higher steering angles, thus covering more cells at the

same time.

2.2 Classification of aerial platforms

Aerial platforms come in many shapes and sizes with widely varying capabilities. Based on these, the systems can be categorised in a number of ways depending on the end goal of the classification effort. For example, aviation regulation can be thought to form a comprehensive risk-based classification framework for the whole spectrum of platforms all the way from small drones and lighter-than-air balloons to heavy manned jet aircraft. On the other hand, these regulatory classifications tend to be very coarse in their breakdown to avoid ambiguity, limiting their applicability for evaluating platforms based on their capabilities rather than their inherent risks.

This is something that can be see for example in the drone regulation of the European Union Aviation Safety Agency (EASA). The framework in the 2020 regulation splits UAS into three distinct operational categories, which are open, specific and certified. The risk model considers four core factors in its evaluation: maximum takeoff mass (MTOM) of the UAS, whether the payload is hazardous, whether the vehicle is flown in visual line-of-sight (VLOS) of the operator and at what altitude [30].

Risk-based approaches tend to be primarily mass-driven. In order to gain a more holistic picture of the platform under evaluation, we may want to introduce some additional factors into the classification. While there are an almost endless list of potential variables to classify a complex system, the top-level categories of performance, payload, system configuration tend to encompass a majority of the ones relevant for different aerial platforms, be they a heavier manned aircraft, lighter-than-air craft or fixed or rotary wing UAV. Figure 4 visualises the classification originally devised by the U.S. Department of Homeland Security in terms of operational altitude and endurance.

In [31], the authors looked at classifying variety of unmanned aerial systems (UAS) platforms and sensor payloads based on their capabilities and applicability for meeting the demands of users in the scientific research sector. The authors adopted a UAS classification framework that draws heavily from earlier military categorizations used by the security establishment in the United States. The framework divides UAS platforms into seven categories based upon characteristics such as size, flight endurance, and capabilities. The categories are in ascending order by mass and performance micro air vehicles (MAV), vertical takeoff or landing craft (VTOL), low altitude short endurance UAS (LASE), close proximity LASE UAS (LASE Close), as well as low, medium and high altitude long endurance UAS (LALE, MALE and HALE). Figure 4 presents the prior categories in terms of MTOM and operational altitude with LASE and LASE Close combined into a single category.

It is worth noting, that the U.S. Department of Defence (DoD) switched to a joint classification scheme for UAS in early 2010s. As described in [32], the classification encompasses all platforms that the different branches had in use when the scheme was introduced. The DoD scheme categorises UAS into five groups based on the MTOM, operational altitude and speed of the platform. Table 2 presents the DoD UAS

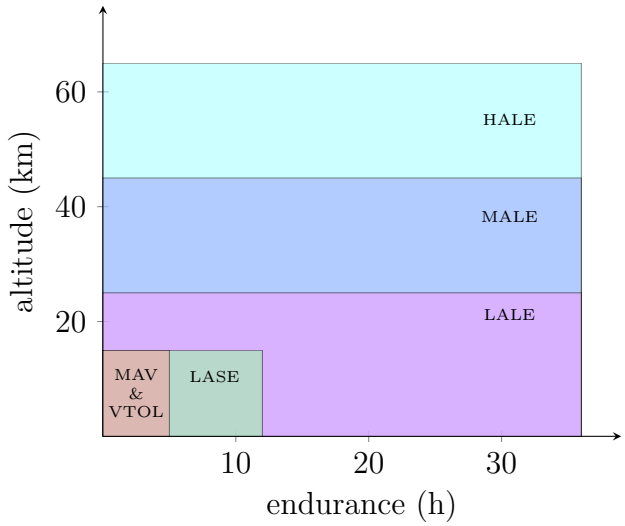

Figure 4: UAS classification in terms of operational altitude (kilometers) and endurance (hours) [31].

groups as they are defined in [32]. The imperial units of the original classification have been converted to metric and rounded for the sake of readability.

In [33], the authors propose a more fine grained classification. While the classification is very detailed in terms of different structural sub-types, the basic approach is still similar to previous classification models following a mass-and-size-based approach. On the highest level, their classification breaks UAS into six categories: normal and small UAVs, and micro-, nano- and pico air vehicles (MAV, NAV and PAV). The mass-and-size top-level classification is complemented by a more fine grained structural configuration based classification. Figure 5 presents the UAV classification in more detail. Third-level categories of rotary wing and Bio NAV / MAV types have been omitted from the figure.

In the broader context of flight operations, which typically encompass takeoff, climb, cruise, turn, descent, and landing, cruising flight assumes significant importance. Civil aircraft spend a substantial duration in this phase, characterized by straight-line flight with constant velocity and altitude, minimizing climbing and descending maneuvers. Manned aircraft performance is fundamentally characterized by a set of equations, addressing key parameters essential for evaluating cruising flight. These equations, including steady-state trim equations, the relationship between drag and thrust with speed, the correlation between speed and angle of attack, and the maximum lift-to-drag ratio, form the foundation for assessing an aircraft's behavior during the cruise phase. Given the dominance of cruising flight over the entire flight envelope, this phase is pivotal for comprehensive understanding of an aircraft's performance. The equations outlined in this section enable the derivation of various relationships critical for evaluating cruising flight performance [34].

Thorough analysis through derivation of equations is typically unnecessary if the goal is to gain general understanding of the performance of different classes of aircraft. Similar to the aforementioned classification frameworks for UAS, manned aircraft

Table 2: UAS classification groups of the U.S. DoD [32].

UAS category	Maximum Gross Takeoff Weight (kg)	Normal Operating Altitude (m)	Speed (IAS, km/h)	Representative UAS
Group 1	0 – 9 kg	<370 AGL	190	WASP III, TACMAV RQ-14A/B Buster, Nighthawk, RQ-11B, FPASS, RQ-16A, Pointer, Aqua/Terra Puma
Group 2	9 – 25 kg	<1000 AGL	<460	ScanEagle, Silver Fox, Aerosonde
Group 3	<600 kg	<5500 MSL	<460	RQ-7B Shadow, RQ-15 Neptune, XPV-1 Tern, XPV-2 Mako
Group 4	>600 kg	<5500 MSL	Any airspeed	MQ-5B Hunter, MQ-8B Fire Scout, MQ-1C Grey Eagle, MQ-1A/B/C Predator
Group 5	>600 kg	>5500 MSL	Any airspeed	MQ-9 Reaper, RQ-4 Global Hawk, RQ-4N Triton

can be categorized through a number of parameters. In [35], the authors propose a very comprehensive synthetic and comparative approach to evaluate both aircraft and rotorcraft. Parameters examined included detailed geometric characteristics for both aircraft and rotorcraft, with former comprising of metrics such as wing span, area, aspect-ratio, sweep angle, dihedral/anhedral angle, thickness and taper ratios, and the latter ones like type of rotor, diameter, number of blades, solidity, rpm, tip Mach numbers. In addition, the authors looked at the aerodynamic characteristics of the platforms under evaluation through the drag coefficients at zero lift and cruise, as well as maximum absolute glide ratio. The performance of different platforms was evaluated through metrics such as wing and disk loading, Mach number, service ceiling, rate of climb, g-limits, MTOM, payload mass and thrust-to-weight ratio.

High altitude balloons are also an interesting platform type when considering their applicability for signals intelligence. These systems are mainly interesting due to

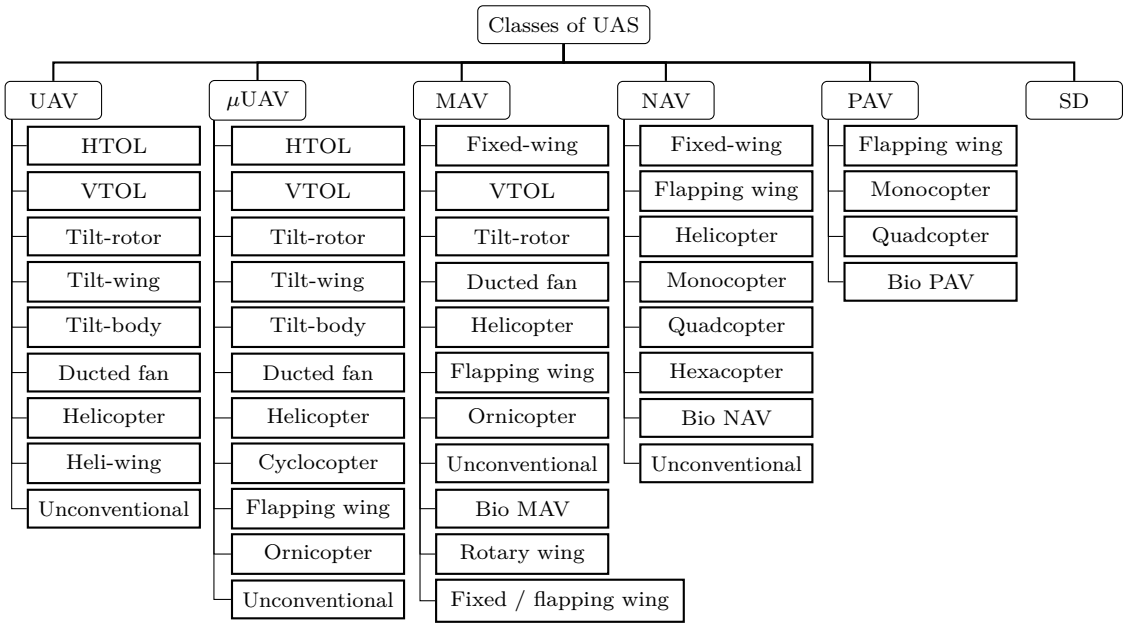

Figure 5: An UAS classification scheme derived from [33].

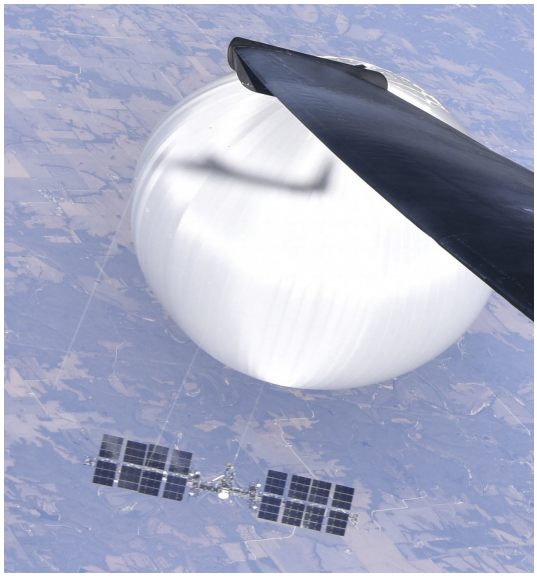

Figure 6: Chinese surveillance balloon over the Central United States as photographed from a U.S. Air Force U-2 on February 3. High altitude balloons have potential for aerial signals intelligence due to their low radar cross section and the wide area of coverage arising from their stratospheric cruising altitude [36].

their low radar cross section and the wide area of coverage enabled by their relatively high stratospheric cruising altitude [36]. Figure 6 shows the Chinese surveillance balloon flting over the Continental United States as photographed from a U.S. Air Force U-2 during an widely reported incident in early 2023.

The goal of the experimental portion of this thesis is to evaluate vulnerability

of VSATs to airborne adversaries. Key factors for the evaluation are the ones that define an aircraft's performance: cruising speed and altitude, as well as payload mass, endurance and maneuverability. The latter is especially interesting, as it can greatly vary between platform types. For example, lighter than air crafts, such as high altitude balloons have relatively limited maneuverability, as they rely on athmospheric air currents to carry them around.

2.3 Communications security

2.3.1 Theory of secure communications channels

Fundamentally, secure communications rely on two core objectives being fulfilled. The intended receiver should be able to recover the original message without errors, while nobody else should be able to acquire any of the contained information. As is customary in cryptography, the transmitter is often referred to as Alice, the receiver as Bob and the eavesdropper as Eve. [37] This core principle of secure communications was formalised by Shannon [38] in his seminal 1949 paper through the notion of perfect secrecy achieved through a one-time pad. Shannon's secrecy system assumes that both the intended recipient and the eavesdropper acquire the encoded codeword without any degradation, i.e. the communication channel is error-free. This theoretical assumption applies very rarely to real world systems, where some noise is almost always present. [37]

Wyner [39] expanded on Shannon's original system by exploring the role of noise in the context of secure communications through the channel model called *degraded wiretap channel* (DWTC). The model assumes a situation where the sender (Alice) attempts to communicate with the legitimate recipient (Bob) over a noisy channel. Simultaneously an eavesdropper (Eve) observes a degraded version of the signal received by the legitimate recipient. [40] Wyner's wiretap channel introduced many mathematical tools for modelling information-theoretic security without the added complexity of fully general channel models. One of these important concepts is the secrecy capacity of the channel, which describes the greatest amount of information that can be confidentially communicated between the legitimate transmitter and receiver from the information-theoretic secrecy perspective. [37]

Csiszár and Körner [41] developed a more general approach that they termed the *broadcast model with confidential messages*.

These seminal works form the foundation for physical layer security research.

Experimental portion of the thesis will examine security of

2.3.2 Signals intelligence: ELINT, COMINT and FISINT

U.S. Department of Defense (DoD) terminology serves as the foundational framework for discussions on diverse facets within the realm of signals intelligence. Essential principles of doctrine, guiding the coordinated and integrated application of U.S. military force, are detailed in Joint Publications (JPs) published by the U.S. Joint Chiefs of Staff. These publications establish foundational doctrinal framework, ensuring standardized procedures for planning, executing, and evaluating military

operations, playing an integral role in facilitating a common understanding and synchronized efforts across various branches of the U.S. military.

Within this landscape, intelligence practices are covered in the JP 2-0 Intelligence Series. JP 2-0 [42], titled *Joint Intelligence* and serving as the keystone document of the series, provides the doctrinal foundation and fundamental principles guiding joint and national intelligence products, services, and assessments in support of joint operations. In JP 2-0, the domain of signals intelligence (SIGINT) is categorized into three distinct subdomains. Communications Intelligence (COMINT) involves gathering intelligence from intercepted foreign communications via radio, wire, or electromagnetic means, extending to encoded imagery. Electronic Intelligence (ELINT) focuses on non-communications emitters like radar, with operational electronic intelligence emphasizing operationally relevant information and technical electronic intelligence delving into technical aspects of the target systems. Lastly, Foreign Instrumentation Signals Intelligence (FISINT) analyzes data from foreign equipment and control systems, offering insights into telemetry, electronic interrogators, and command systems, providing a comprehensive understanding of foreign technological capabilities. In other SIGINT methodologies [43], FISINT is often grouped together into ELINT when its definition is taken in the broader non-communications sense.

Signals intelligence (SIGINT) is intelligence gathering through the exploitation of communication systems and noncommunications emitters. Based on the nature of the target system, the discipline of SIGINT can be further subdivided into the sub-disciplines of communications intelligence (COMINT) and electronic intelligence (ELINT) [44] [JP 1-02, JP 2-0 (2013), JP 3-85].

Considering satellite communication systems, the two disciplines of signals intelligence provide a wide range of tools for intelligence gathering at different levels of abstraction. On the most resource-intense end, we have the interception and extraction of user traffic, the defined scope of COMINT. However, less sophisticated methods, such as signal detection and fingerprinting, direction finding (DF) and radiopositiong may still yield valuable insights into the nature of the utilized systems, the user organisations, use patterns. As no

Interception of user traffic in satellite networks falls under the discipline COMINT. On based on methods such as time of

2.3.3 Electronic warfare: attack, protection and support

2	123

Figure 7: Electronic warfare taxonomy based on [43].

EW involves military actions leveraging Electromagnetic (EM) and Directed Energy (DE) to either control the Electromagnetic Spectrum (EMS) or to launch attacks against the enemy. This multifaceted domain comprises three distinct divisions: Electronic Attack (EA), Electromagnetic Support (ES), and Electromagnetic Protection (EP).

ES involves actions to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy. It serves immediate threat recognition, aids in targeting, contributes to planning, and supports the conduct of future operations on a tactical level. Despite the similarities, ES is a separate discipline from SIGINT. The distinction between the two is delineated by purpose, scope, and context. While ES is focused on immediate operational needs, it shares commonalities with SIGINT, with both potentially using the same assets to simultaneously collect information meeting operational and intelligence requirements. To quote JP3-85 [45], "it can be said that information collected from the EMS has “two lives.” The first is as ES, unprocessed information used by operational forces to develop and maintain SA for an operationally defined period of time. The second is as SIGINT, retained and processed under appropriate intelligence authorities in response to specified intelligence requirements."

Electronic Attack (EA) constitutes another key facet of EW, deploying electromagnetic energy, directed energy, or antiradiation weapons to attack enemy personnel, facilities, or equipment. The intent is to degrade, neutralize, or destroy the combat capability of the adversary. This division, also known as EA, is considered a form of fires within the military context, illustrating its role in directly influencing and diminishing enemy combat effectiveness.

The third division, Electromagnetic Protection (EP), encompasses actions taken to shield personnel, facilities, and equipment from the detrimental effects of friendly or enemy use of the electromagnetic spectrum. EP is essential for maintaining the integrity and functionality of friendly combat capability in the face of electromagnetic threats.

On the practical side, ES is often intelligence gathering and dissemination while EA is direct actions like jamming. EP not concerned with affecting a target system or gaining information, but rather protecting systems from external elec threats.

2.3.4 TRANSEC and physical layer constraints

2.3.5 Signal detection

2.3.6 Direction finding and radiopositioning

Geolocating fixed VSAT terminals implemented as phased arrays, different direction finding techniques can be assessed for their suitability based on several factors. Some of the modern techniques include:

Angle of Arrival (AoA): AoA techniques can be suitable for geolocating VSAT terminals. By measuring the angles from which the signals arrive at the aircraft's direction finding array, the azimuth and elevation of the terminals can be estimated. AoA techniques like beamforming, MUSIC, or ESPRIT can be effective in estimating the angles of arrival, especially if the phased array terminals have discernible sidelobes or beam characteristics.

Time Difference of Arrival (TDOA): TDOA relies on measuring the time delays between signals received at multiple spatially separated sensors.

Frequency Difference of Arrival (FDOA): FDOA relies on measuring the frequency

differences of signals arriving at different sensors or antennas. FDOA techniques may provide useful information if the signals have specific frequency characteristics or modulation patterns that can be exploited.

Beamforming: Since phased array VSATs employ beamforming, the listeners direction finding array can analyze the received signals' phase and amplitude information to estimate the direction of arrival.

Additionally, multiple techinques can be combined into a hybrid approach if the complexity and capabilities of the direction finding array permit. For example, combining AoA and beamforming techniques can enhance the accuracy and robustness of geolocation estimates, especially if the phased array terminals exhibit unique radiation patterns or have challenging sidelobe characteristics.

2.4 Critical communications

2.4.1 Narrowband-to-broadband evolution

Critical communications are entering a major paradigm shift. Thus far, national authorities have relied globally on dedicated, purpose-built narrowband technologies such as TETRA, Tetrapol and P25 in their operational communications. Broadband standardisation initiated by The Critical Communications Association (TCCA) Critical Communications Broadband Group (CCBG) in 2012 and developed in a working group of 3GPP's Technical Specification Group since 2015 have adapted the commercial 4G/5G standards to the strict requirements of critical communications. Roll-out of systems built around these standards is currently ongoing in many countries, for example through migration projects such as VIRVE2 in Finland, RRF in France or ESN in the United Kingdom.

The evolution is not limited to just wireless communication technology. In the public safety context, the shift to the more versatile broadband ecosystem enables transitioning from the current voice-only operating model to a more diverse one with voice, video and data capabilities. The higher versatility necessitates reliable access to magnitudes greater bandwidth for them to function. In narrowband networks, building coverage was often the main factor to be considered. On the other hand, ensuring adequate capacity alongside coverage requires additional consideration in broadband networks [46].

The broadband transition also means a shift from custom technology solutions to more mainstream ones. Critical communications segment places strict requirements on availability, reliability, security, and coverage. For example, the coverage requirement for a national critical communications network can be close to 100 percent of the geographic coverage, while commercial networks are built based on a business case primarily driven by population density. In general, this leads to coverage figures far from 100 percent [46].

2.4.2 Use cases and scenarios

Critical communications service operators see satellite systems as a complementary coverage and capacity solution, where the main use cases can be characterised through how long lasting and planned the events requiring response are. On a high level, the coverage and capacity needs can be either permanent, planned temporary or unplanned temporary in nature. Prevalent geographic conditions and duration of active use tend to be the determining factors that decide which of the cases is the most applicable in each situation.

Permanent applications tend to be the most obivious when it comes to the typical locations. They encompass the traditionally difficult-to-serve regions. For example, sparcely populated rural areas and maritime settings have been typically rather poorly served by mobile network operators due to their limited commercial potential. On the other hand, the temporary use cases tend to be more varied in terms of the potential types of locations. While coverage augmentation is typically still needed only in underserved locations, capacity needs may arise in areas with normally sufficient

terrestrial coverage. For example, large events are a typical example of temporary use cases that can be planned for in advance. These include mass events like sports and concerts and political events like state visits and summits [47–49]. Unplanned events can be both man-made or acts of nature and can range from localised to widespread in affected area. For example, natural disasters, like earthquakes, floods, or forest fires, can lead to widespread infrastructure damage, while man-made disasters like airplane crashes or multiple vehicle collisions are usually more limited in terms of the affected area [50, 51].

Another differenciating factor of the above mentioned events is their forecastability and typical duration. Both planned and unplanned events can last from days to months, with the duration having different implications for the choice of the best suited technological solution. Satellite connectivity may even be needed permanently when it comes to backhaul applications in very remote locations to where building terrestrial connectivity might be simply unfeasible. The cut to planned and unplanned events is also not really black-and-white, but these notions exist on a spectrum of different tones of grey. For example, natural disasters such as earthquakes might cause unplanned damage that requires immediate response. On the other hand, some weather events, such as hurricanes and forest fires may be forecasted to differing extents.

All in all, satellite connectivity does not replace the traditional terrestrial networks but complements them. If deployed to their envisioned state, broadband satellite systems may work as a cost-efficient way to serve these regions and events. Thanks to their truly global coverage pattern, while the lower user density in these regions is still within the load carrying capacity of these networks.

2.4.3 Requirements

Public Safety users have stringent data security requirements for their communications due to the sensitive nature of these exchanges. Satellite links bring new considerations in the transit of the data through other nations, as the networks are inherently global in nature. In the commercial operating model the constellations downlink data at sites that are most convenient for their operation, which means that the data will often transit through other sovereign countries before arriving at its final destination. Over-the-air transmission of data presents also questions on the jamming resilience of the satellite links.

This poses challenges during situations where a nation is under an external threat, be it a military conflict or an act of a rogue organisation, as sensitive operational information needs to remain only in the hands of its intended users. In addition to these general architectural considerations, the technical solutions themselves should be verifiable on the national or at least at the EU level for both the hardware and software.

Preparedness is a key aspect in the operating model of public safety organisations. It covers the actions required for ensuring the smooth execution of tasks central to the overall safety of a nation in large emergency situations and societal disruptions. Preparedness actions include contingency planning, continuity management, advance

preparations, training of operatives and readiness exercises. The concept revolves around the goal of anticipating threats rather than having to react to them [12].

In the case of public safety communications, this leads to high requirements for availability even in a state of emergency. Similarly to more traditional terrestrial solutions, the requirements apply also to the emerging satellite links, which will most likely serve as a back-up solution in the case of larger scale failures of other options.

Satellite links are likely the best suited to natural disasters and major accidents but open questions remain related to human-made threat situations, like terrorist attacks and military conflicts, where external actors may deliberately interfere with the communications links. This raises questions on the political regimes where these current and future constellations are owned and operated. Nationally controlled satellite communications solutions would be the most optimal but are unfeasible for most of the World's nations to implement. This is due to the immense capital requirements, especially when considering LEO options, which require at minimum hundreds and often thousands of satellites.

These budgetary requirements lead to a situation where most nations need to rely on satellite services that are provided by operators from foreign countries. As discussed later, many of the emerging new operators are either US or UK based, while the EU has also been considering entering the constellation sector with its own alternative. In the EU member state context the latter is probably the most attractive option, especially from the point of critical communications. Control over the constellation and its ground segment will be as close to the national level as is feasible with the capital intensive satellite systems. US and UK based solutions might be also in this sense allowable but are likely to require significant legislative work when used by governmental public safety users.

Straightforward usability of the systems is highly critical from the perspective of public safety users based on the interviews with Finnish Public Safety actors. The success rate in emergency situations depends heavily on the timeliness of the response, which means that the communication systems used in field activities need to be available on a standby-basis. Thus, the future satellite link would need to be highly integrated with the existing communications infrastructure for it to be effective, so that it can be used when necessary.

Considering these usability requirements, an ideal user terminal would be a handset with integrated satellite communication capabilities, but this is not feasible with the current satellite terminal sizes. The more feasible alternative in the near-term would be the integration of the terminal to the vehicles used by the authorities in daily activities.

In addition to conveniently sized and well integrated user terminals, satellite services should be agnostic to the applications that are run through the link they provide. Currently used applications include PTT, data and video, while in future the systems should be able to accommodate more complex applications, like the verified positioning services provided by the Galileo Public Regulated Service (PRS). This may though require special arrangements in timing critical applications, as satellite systems have longer end-to-end delay times compared to terrestrial systems.

Cost considerations are another important point of discussion as they have been a

limiting factor for the adoption of the existing satellite services. The new constellations need to achieve significantly lower per user costs for the solutions to gain widespread adoption. The public safety sector is a niche market from the point of view of the constellation operators, which is especially the case for smaller countries like Finland. Volume based pricing models are a possible way of achieving cost advantages but are likely to require the tendering processes to include multiple possible user groups. One straightforward model for providing satellite access to the user organisations could be to include it to the services provided by a national critical communications operator (e.g. Erillisverkot in Finland).

For the solutions to become widely used, their monthly cost should be tens of euros for an individual user terminal. If implemented as a vehicular solution, these kinds of monthly costs would lead to a country wide cost in millions of euros.

2.4.4 Technical considerations

Implementation-wise, permanent use cases are maybe the most straight forward, as they are can be implemented as a simple FSS backhaul link of an individual base station site. Direct satellite connectivity is also something that may be feasible in these regions long-term, but as was discussed in chapter 2.1.2, its technological maturity remains relatively low.

Implementation-wise, satellite networks are in the short-to-medium term envisioned to integrate into the terrestrial networks through portable tactical bubbles, where the satellite link serves as a backhaul solution for a local (?100 meters to kilometers?) wireless connectivity bubble. In practice, current equipment form factor and cost supports best a vehicular deployment model. For example the French RRF envisions satellite networks as one backhaul option for its vehicular relay (*relais véhiculaire*), an emergency vehicle with a tactical bubble for local coverage and capacity. On the other hand, integration point for satellite systems in the Finnish VIRVE2 has been envisioned as command vehicles of fire, rescue and police forces [**?**, 46].

Long-term, evolution towards direct-to-smartphone type solutions is a potential development path. 3GPP has been working towards integrating satellite connectivity as one of the options in the 5G Non-terrestial networks (NTN), a development item also present on the longer-reaching 6G roadmaps [**?**, **?**]. It is though worth noting, that these solutions remain rather low in terms of their technological maturity. In-orbit demonstrations of the technology have been very limited in number and work has focused more on the theoretical standardisation work

In this section, we address the important security features of the TETRA network. Here the scope of coverage spans the authentication, encryption mechanisms, and the key management of TETRA. It dictates that a secure communication network needs to provide (Stavroulakis, 2007):

Confidentiality Integrity Reliability Non-repudiation Authentication.

6.7.8.1 Confidentiality

Only authorized personnel or people should have access to the information being passed along.

6.7.8.2 Integrity

Table 3: Essential requirements for tactical bubbles [52].

Communication type	Requirement category	Identified requirements
Generic	Availability	99% to 99.999%
	Start-up time	0 to few minutes
	Configuration efforts	Zero-configuration
Combined user traffic (avg.)	Downlink / user	50 Mbps
	Uplink / user	25 Mbps
Push to talk	Packet delay	75 ms
Group video	Packet delay	100 ms
Virtual reality (4K GC video)	Data rate	50 to 200 Mbps
	Latency	<16 ms
Sensor data	Sensor amount / cell	0 to massive
Machine remote control (UAV)	Latency	40 ms to 1 s

This refers to the requirement that states that only authorized users need to be able to make any modifications to the information in exchange.

6.7.8.3 Reliability

This refers to the requirement that the resources and the services are not denied and are available to the authorized users to accomplish various tasks.

6.7.8.4 Non-repudiation

This requires that the sender cannot deny that he/she sent the message. 6.7.8.5 Authentication

This refers to the requirement that the sender's identity is verifiable by the recipient.

3 Research material and methods

3.1 Methodology

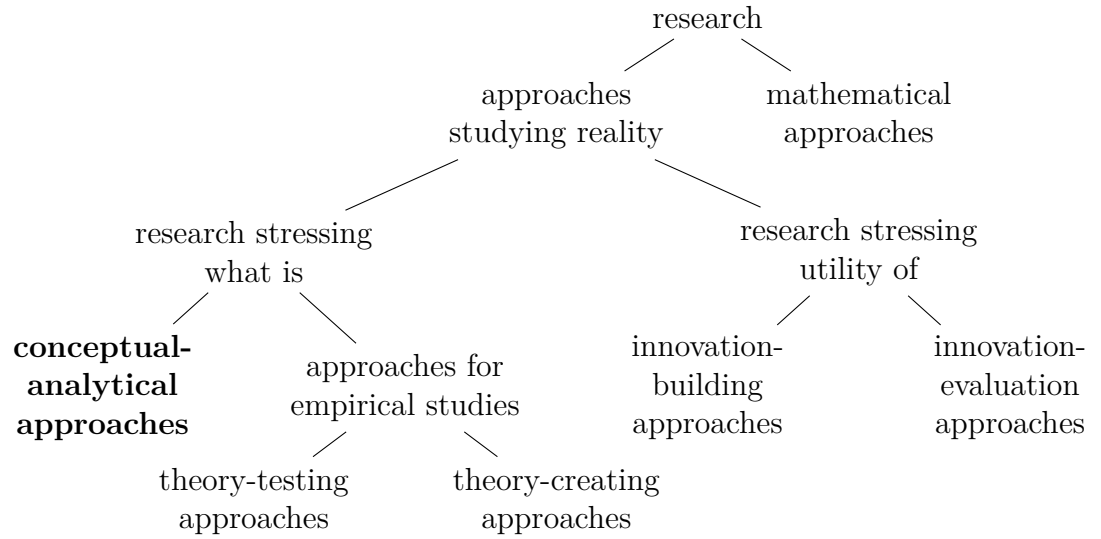

Figure 8: Research approach taxonomy of Järvinen [53, 54]. Conceptual-analytical approach followed in this thesis is highlighted.

Järvinen [53, 54] offers a comprehensive framework for categorizing research approaches, building upon the foundation laid by March and Smith [55]. This taxonomy constitutes six distinct research approaches: mathematical, conceptual-analytical, theory-testing, theory-creating, innovation-building, and innovation-evaluating. Mathematical approaches primarily engage with abstract concepts detached from the constraints of the real world, while research approaches studying reality fall into two main categories—natural and social science approaches (conceptual-analytical, theory-testing, and theory-creating) and design science approaches (innovation-building and innovation-evaluating). The taxonomy proposed by Järvinen in [53, 54] is presented in figure 8.

Within the taxonomy, this thesis falls under the conceptual-analytical research approach, the scope being technology-oriented in nature. This approach relies on logical reasoning and draws extensively from prior research and established theories. Conceptual-analytical approaches within the natural and social sciences do not necessarily rely on empirical data, while theory-testing and theory-creating approaches use data to either validate existing theories or formulate new ones. The primary objective of conceptual-analytical research is to generate new creating theoretical concepts or analysing existing theories.

In practical terms, the modelling approach in this thesis is grounded on theoretical background of RF systems and more specifically concepts related to electronic warfare and signals intelligence. Threat model builds upon theory discussed in [43] and [56]. Target systems are explored through a parametric study of an analyitical model comprised of multiple submodels that incorporate relevant parameters for aerial

signals intelligence platforms and both space and ground segments of a satellite communications system.

3.2 Data sources

4 Results

4.1 Threat model

The core goal of this thesis is to assess whether the presence of airborne eavesdroppers poses a risk to the uplink communications of emerging NGSO VSAT networks. The research applies quantitative analysis by building a threat model focusing on a Walker-type LEO megaconstellation, fixed Very Small Aperture Terminals (VSAT) and airborne eavesdroppers. The threat model is built around a set of four smaller submodels, each examining analytically a relevant dependent variable against a number of independent ones. The models are first introduced in a deductive manner tying reality to the underlying theoretical concepts. Individual submodels are then parametrically studied in a range of starting conditions mirroring the relevant characteristics of the platforms under evaluation. Descriptions for the submodels are given in table 4 while their independent and dependent variables of the parametric study are introduced in table 5.

The models explore the target system from first principles using geometric and kinematic analysis, as well as link budgets based on an example hardware configuration. First principles thinking is a powerful problem-solving approach that involves breaking down a problem or a concept into its elemental parts. In this sense, each submodel helps us understand potential strengths and vulnerability of different satcom systems through an elemental understanding of the underlying physical phenomena.

Critical communications users place high expectations on the communications solutions that they utilise. Satcom solutions have seen previously somewhat limited especially in the public safety sector, while at the same time commercial systems have turned out to be not the most robust when it comes to to fundamental concepts of security, such as confidentiality, integrity and availability. With the recent drive to integrate satcom into both commercial and critical use cases, it is paramount to understand the underlying factors of the systems. Physics-driven analysis helps us to evaluate the limits of a systems in a way that allows for sufficient risk mitigations to be engineered.

Table 4: Descriptions for the sub-models.

sub-model	target metric
1	maximum interception range
2a	beam tracking potential, equatorial orbits
2b	beam tracking potential, inclined orbits
3	listening window
4	jamming link budget

Submodel 1 examines the maximum interception range of a fixed satellite terminal. This metric helps us to evaluate the potential maximal area where a single satellite terminal is vulnerable to airborne eavesdroppers. Airborne platforms may listen

to transmissions from great distances, for example flying in an airspace of another country. Submodels 2 and 3 examine an aircraft's ability to track an UT's RF beam. VSATs have typically a relatively narrow beam pattern of a few degrees of half power beamwidth. Relative motion between the beam and an intercepting aircraft is a major consideration when it comes to evaluating the vulnerability of different satellite systems. Submodel 4 examines the a jammer's ability to interfere with a legitimate UT interfacing with a LEO megaconstellation. Link budget for an uplink connection from an UT to a satellite is computed. In the scenario, the jammer competes with the legitimate transmitter in RF signal power received by the satellite.

Table 5: Independent and dependent variables of the sub-models.

Sub-model	Dependent variable	Independent variables
1	interception range (m)	minimum elevation angle (deg) eavesdropper's altitude (m)
2a	velocity of the sub-satellite point, equatorial (m/s)	orbital altitude (m)
2b	velocity of the sub-satellite point, inclined (m/s)	orbital altitude (m) inclination (deg)
3	listening window (s)	orbital altitude (m) inclination (deg) eavesdropper's velocity (m/s)
4	required jamming power (dBW)	target SJNR at RX (dB)

4.2 Submodel 1: Maximum interception range

In order to eavesdrop a target transmitter, an eavesdropper need to be able to intercept sufficiently strong uplink signal. Being firmly out of range of an earth station, in other words inside a white zone, is the most fundamental limit to an eavesdropper's ability to eavesdrop. This can be thought as arise where eavesdropping is either simply impossible or a very tough uphill battle:

1. The VSAT earth station falls behind the radio horizon of the eavesdropper.
2. The eavesdropper falls outside the main lobe of the VSAT earth station.

As presented in appendix A, broadband VSAT systems both existing and under development tend to operate in the Ku and Ka bands (12–18 and 26.5–40 GHz respectively), with the former being the more commonly used in user links between the orbiting satellite and user terminal and vice-versa, although some systems, such as Amazon's Project Kuiper deviate from this "rule". In terms frequencies, both bands fall under super high (SHF, 3-30 GHz) to extremely high frequencies (EHF, 30-300 GHz), where the principal propagation mode is line-of-sight propagation. In

this mode, the radio horizon of a transmitter can be derived from the Pythagorean theorem, assuming a perfectly spherical planetary body.

Going into the geometry of the problem, line-of-sight distance d and radius of the body R form the legs of a right triangle, while the transmitter's distance from the centre of the body $(R + h)$ is the hypotenuse [57]. The relationship between the quantities is visualised in figure **??**.

$$d^2 = (R + h)^2 - R^2 = 2R \cdot h + h^2$$

In case of the Earth, the height of both surface-bound and airborne transmitters h is rather insignificant compared to the radius of the body R. Thus, we can simplify the line-of-sight equation to

$$d \approx \sqrt{2R \cdot h} \tag{1}$$

It is worth noting that equation (1) applies only in vacuum. Vertical pressure variation of an athmosphere refracts passing electromagnetic waves. In practice, the waves deviate from a straight line down towards the surface. This deviation can be accounted for by applying a factor k to equation (1). In case of the Earth, an effective radius of 4/3 is usually applied [57].

$$d \approx \sqrt{2k \cdot R \cdot h} \tag{2}$$

Radio horizon allows us to examine situations where the transmitting antenna is either isotropic or pointed deliberately in the direction of the horizon. This is not always the case with highly directional VSAT terminals, thus requiring additional factors being taken into account. Here, one of the most important parameters is the minimum elevation angle of the satellite system in question. Similar to radio horizon, maximum VSAT interception range can be examined through a trigonometric approximation model.

As discussed regarding the characteristics of the terminals, typical minimum elevation angles range from 20 to 55 degrees in the recent broadband megaconstellations in LEO. As the operational altitude of the eavesdropper is known, theoretical maximum interception range can be computed for a range of the minimum elevation angles. The measurands form an orthogonal triangle with the minimum elevation as the acute angle opposite to the height of the triangle. The operational altitude of the eavesdropper is the height of the triangle, while the base is formed by the theoretical interception range of the system. Lastly, the hypotenuse is the line-of-sight (LOS) distance between the VSAT site and the airborne eavesdropper.

Trigonometric tangent function of the interception range triangle is

$$\tan(e_{Alice}) = \frac{h_{Eve}}{d_{Eve}} \tag{3}$$

where e_{Alice} is the minimum elevation angle of the user terminal, h_{Eve} is the operational altitude of the intercepting airborne platform and d_{Eve} is its distance from Alice on the ground, in essence the interception range. Rearranging (3) for d_{Eve} gives

$$d_{Eve} = \frac{h_{Eve}}{\tan(e_{Alice})} \tag{4}$$

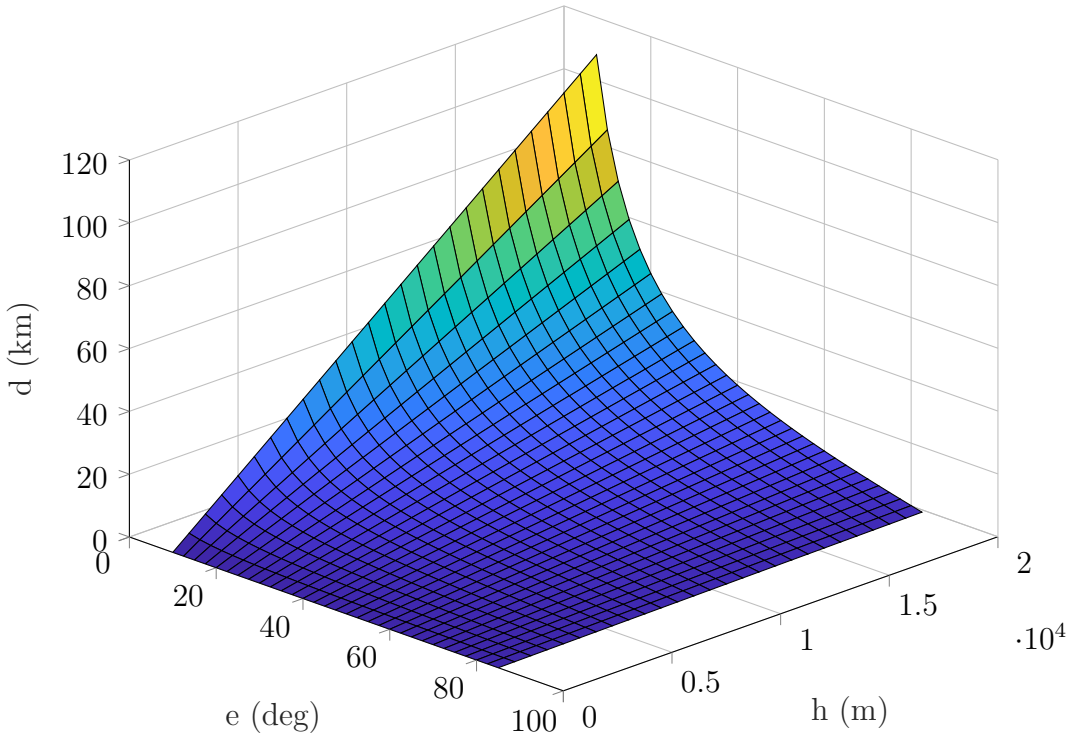

Figure 9: Interception range (d) as a function of minimum elevation angle (e) and operational altitude of the eavesdropper (h).

Figure 9 shows the interception range d_{Eve} in the range $e_{Alice} = [10°, 85°], h_{Eve} = [100, 20000]$. In the resulting 3D plot, the dependent variable or the interception range (d_{Eve}) of the airborne eavesdropper is on the vertical axis. Independent variables or the minimum elevation angle of the terminal (e_{Alice}) and opertional altitude of the airborne eavesdropper (h_{Eve}) are on the horizontal axes.

The convex surface exhebits linear growth in relation to altitude h_{Eve} and accelerating tangential growth in relation to e_{Alice}. Therefore, we can deduce that the minimum elevation angle is in most cases the driving factor of the maximum interception range of a VSAT ground station. The influence of h_{Eve} on d_{Eve} is markedly smaller but still significant, especially when considering terminals with small e_{Alice}. The tangent function has asymptotes at $e_{Alice} = \pi/2 + n\pi$. Within the given limits, the asymptotes are not reached and the resulting surface is smooth and continuous.

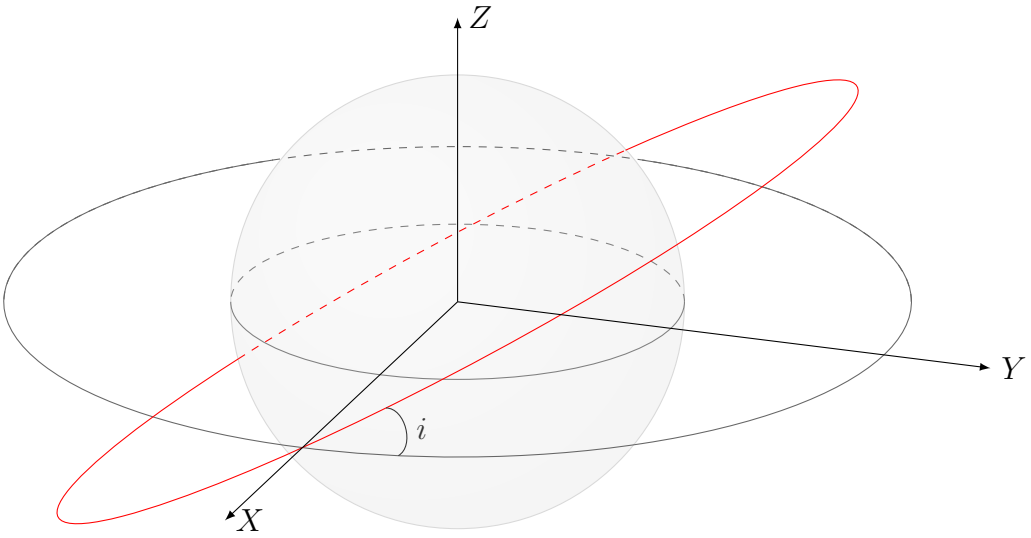

Figure 10: Geometry of a circular Earth orbit.

4.3 Submodel 2a: Beam tracking potential in equatorial orbits

In addition to being aligned along the line-of-sight of the VSAT's main lobe, the eavesdropper needs to be able to intercept sufficiently long transmission to be able to This time dimension brings another point to consider when evaluating the risk of eavesdropping. Different durations of interception have varying implications for the legitimate transmitter. As an practical example, millisecond-level signal capture may be enough for DF applications, while in COMINT monitoring the signal for longer periods ranging all the way from seconds to days would be useful for gathering enough data.

Maximum duration of signal interception is set by the ability of the airborne platform to track the main lobe of the earth station. The beam movement is primarily driven by the motion of the receiving satellite in orbit, which is in turn governed by Kepler's laws of orbital motion. Tracking capability of the aircraft can be evaluated by analysing the velocity of the sub-satellite point at the eavesdropper's operational altitude (point x on figure 10). If this velocity exceeds the cruise speed of the eavesdropper, the airborne platform is not able to continuously follow the uplink RF beam, which limits the time window into individual satellite passes.

Communication satellites reside often in circular orbits, which are a special case when evaluating Kepler's laws of orbital motion. Here, the velocity of the sub-satellite point can be computed by solving Kepler's third law for the orbital velocity at a set altitude. In equatorial orbits, Earth's rotation can be directly substracted from the angular velocity of the satellite, as both share roughly the same rotational axis.

$$T^2 = (\frac{4\pi^2}{GM})r^3 \tag{5}$$

where T is the orbital period, G is the gravitational constant, M is the mass of

the orbited body and r is the radius of the orbit

In essence, the aircraft can be modeled as a low-flying athmospheric satellite. This allows for the same equations to be used in modeling its kinematic characteristics. Solving the required velocity for successful beam tracking can be computed by equating the required orbital period of the aircraft to the one of the space-borne satellite.

Orbital period is related to the angular velocity of the satellite ω_{sat} through the equation

$$\omega_{sat} = \frac{2\pi}{T} \tag{6}$$

which can be used to solve the tangential velocity component at a set altitude v_r

$$v_r = \omega r \tag{7}$$

As $\omega_{sat} = \omega_{air}$ in the case that the aircraft is able to continuosly track the satellite, the velocity of the sub-satellite point at the cruising altitude of the aircraft $v_{r,air}$ can be solved by combining equations (5), (6) and (7). Rearranging Kepler's third law to solve for $v_{r,air}$ gives

$$v_{r,air} = r_{air}\sqrt{\frac{GM_E}{r_{sat}^3}} \tag{8}$$

Variables r_{air} and r_{sat} are the orbital radiuses of the eavesdropping aircraft and the receiving satellite measured from the center of the Earth while M_E is the mass of the Earth. Equation (8) gives $v_{r,air}$ in the ECI coordinate frame. To compute the actual movement of the sub-satellite point relative to the surface of the Earth, the velocity figure needs to be converted to the ECF coordinate system. For circular equatorial orbits, this can be simply achieved by substracting the spin of the Earth from $v_{r,air}$.

$$v_{r,ECF} = v_{r,air} - \omega_E r_{air} \tag{9}$$

ω_E is the angular velocity of the Earth at the equator.

Figure 11 shows the sub-satellite velocity ($v_{r,air}$) of a satellite in equatorial orbit as a function of orbital height $h_{sat} = r_{sat} - R_E$, where R_E is the radius of the Earth. Velocities are examined in orbits ranging from LEO to GEO, which corresponds to the range $h_{sat} = [5 \cdot 10^5, 3.7 \cdot 10^7]$. In the resulting graph, the dependent variable or the sub-satellite velocity ($v_{r,air}$) is on the vertical axis, while the independent variable of the orbital height h_{sat} is on the horizontal axis. The graph can be observed approaching the rotational velocity of the Earth when h_{sat} approaches the height of GEO 36000 km. As the graph is computed in the ECF coordinate frame, we can se sub-satellite velocity approaching zero, which means that the satellite appears fixed in its position in the sky. Cubically decreasing nature of v_{sat} leads to radically higher values for LEO with v_{sat} values ranging roughly between 5 and 7 km/s in orbital altitudes between $h_{sat} = [5 \cdot 10^5, 2 \cdot 10^6]$.

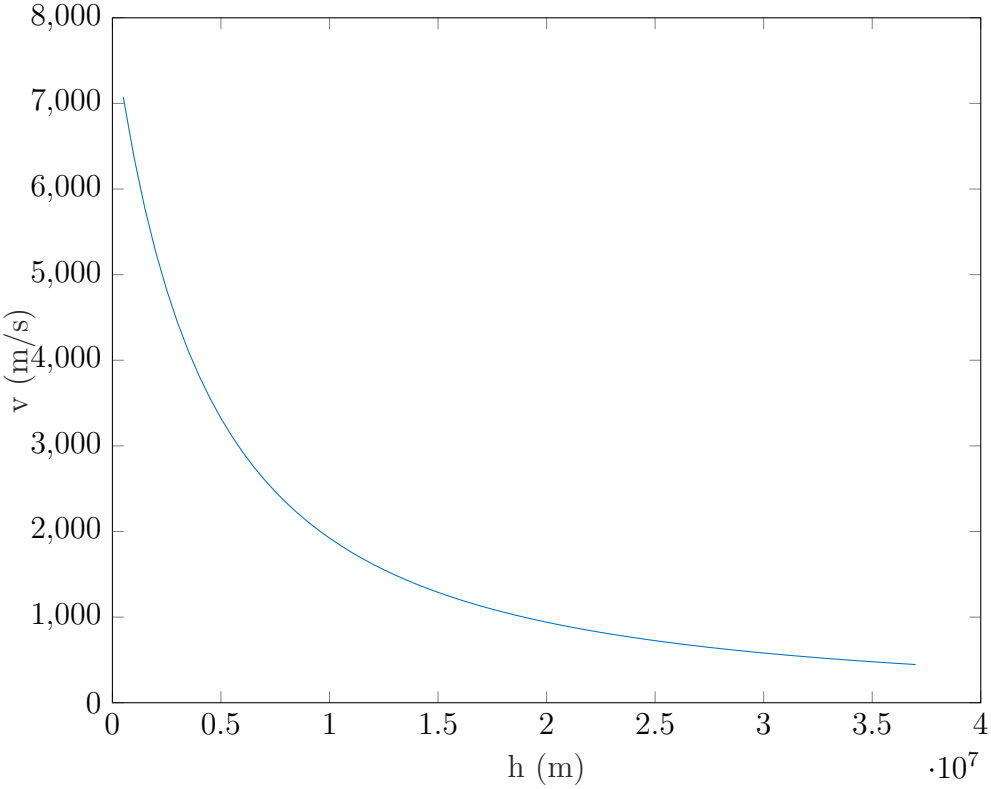

Figure 11: Sub-satellite velocity as a function of orbital altitude (m) in equatiorial orbits.

4.4 Submodel 2b: Beam tracking potential in inclined orbits

Circular equatorial orbits are a good starting point for listening window analysis but their real world applications are somewhat in limited when considering relationship of orbital altitude to coverage and latency. As discussed in chapter 2.1.2, modern satellite megaconstellations, such as the systems in appendix A, aim to achieve worldwide coverage by placing a number of satellites into inclined circular Earth orbits. Common configurations include the Walker Star and Delta constellation configurations, the advantages and disadvantages of which are discussed in more detail in the aforementioned chapter.

The same analysis methods remain valid for inclined orbits but some additional factors need to be considered. Equatorial orbits have only a single velocity component parallel to the xy-plane in both ECI and ECF coordinate frames. On the other hand, any inclination induces additional velocity component perpendicular to this original equatorial component. This velocity component is visualised by v_z in figure **??**.

Transitioning from the simple scalar representation into a vector space makes analyzing inclined orbital motion less cumbersome. Here, angular velocity is a very useful abstraction, as it allows to sum different rotational speed components together. As angular velocity does not vary in in circular motion, examining the magnitude of the sum of the angular velocity vectors allows us to gauge the tracking potential of

differently inclined orbits at the desired range of altitudes.

The ECI coordinate frame is a natural starting point for evaluating orbital motion. Angular velocity pseudovector of a circular orbit follows the right hand rule, being perpendicular to the rotational plane. Rotational motion in the equatorial plane can be represented with angular velocity pseudovector $\vec{\boldsymbol{\omega}} = [0, 0, \omega]^T$. Inclined orbits can be generated by rotating this equatorial orbit about its diameter, which can be achieved with multiplying the pseudovector with a suitable three-dimensional rotational matrix. To rotate the orbits about the y-axis of the ECI coordinate frame by θ degrees, rotation matrix $\boldsymbol{R_y}$ can be used.

$$\boldsymbol{R_y}(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Multiplying the vector by matrix $\boldsymbol{R_y}(\theta)$ and substracting the rotation vector of the Earth gives angular velocity vector in the ECF coordinate frame. This can be in turn be converted to the velocity of the sub-satellite by taking the norm of the angular velocity pseudovector

$$\omega_{ECF} = ||\boldsymbol{R_y}(\theta)\ \vec{\boldsymbol{\omega_{sat,i}}} - \vec{\boldsymbol{\omega_E}}||$$

ω_{ECF} is the scalar angular velocity of the satellite in the ECF coordinate frame. $\vec{\boldsymbol{\omega_{sat,i}}}$ and $\vec{\boldsymbol{\omega_E}}$ are the angular velocity vectors of the inclined satellite orbit and the spin of the Earth. Finally, the sub-satellite velocity figure can be solved based on the scalar angular velocity by applying equation (7), as the altitude of the airborne platform h_{air} and the mean radius of the Earth R_E are known.

$$v_{air} = \omega_{ECF}\ (h_{air} + R_E) \tag{10}$$

4.5 Sub-model 3: Listening window

Listening window is the time that an airborne eavesdropper is able to intercept the uplink RF transmission from a user terminal on the ground. Analysing this window is somewhat more complex in terms of the model required and potential input parameters that need to be considered. On a high level, the window is primarily influenced by the relative motion between the uplink RF beam of the terminal and the kinematic characteristics of the airborne eavesdropper. The latter include qualities such as cruise speed, operational altitude, manoeuvrability and controllability. They define the ability of the aircraft to keep a lock on the moving RF beam. These are in turn defined by the characteristics of the platform, a topic discussed in more detail in section 2.2. As demonstrated by the inclination-orbital altitude analysis, aircraft kinematics have very little effect at LEO satellite altitudes ranging from hundreds to couple thousand kilometers. In practice, the great disparity between the velocities makes it possible to abstract away the movement of the aircraft and assume it to be stationary for the sake of analysis.

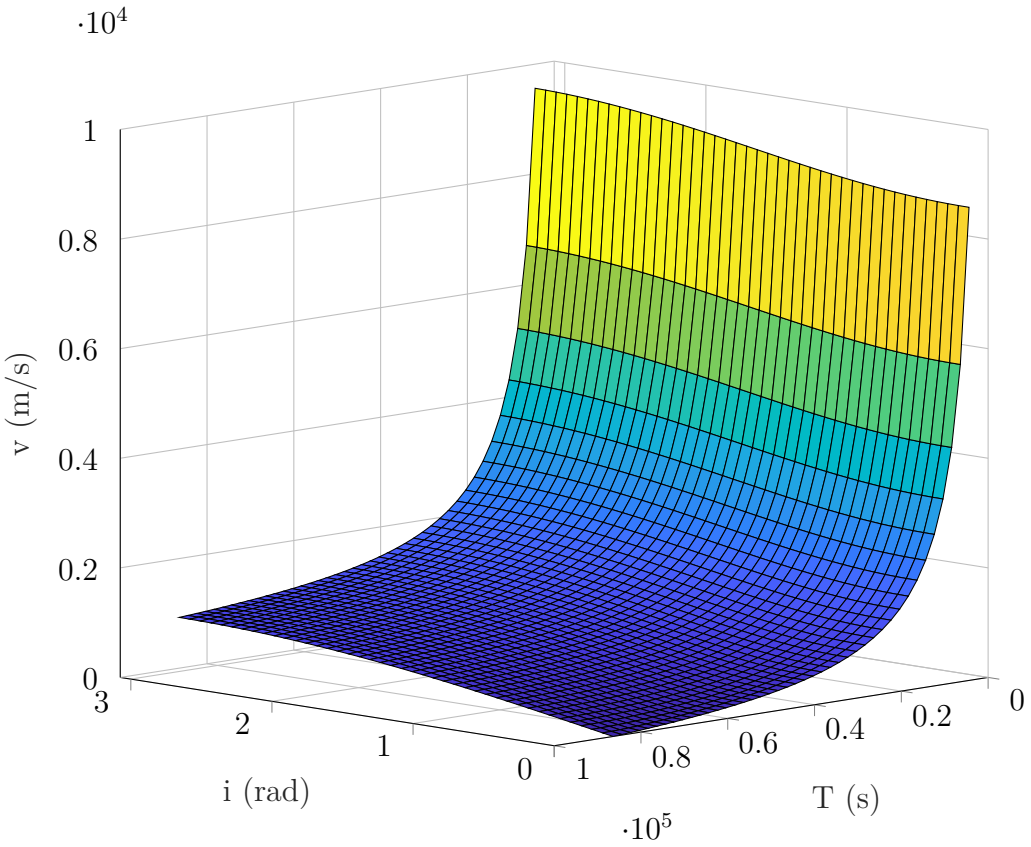

Figure 12: Sub-satellite velocity (m/s) as a function of orbital altitude (m) and inclination (rad KORJAA ASTEET).

Assuming a stationary eavesdropper, the listening window t_{pass} can be computed by dividing the beamwidth of the satellite terminal θ_{beam} with the angular velocity of the satellite in the ECF coordinate frame ω_{ECF}.

$$t_{pass} = \frac{\theta_{beam}}{\omega_{ECF}} \tag{11}$$

Evaluation in smaller domain, $T_{orbit} = [5400, 42400]$. Around GEO grows to infinity as the sub-satellite velocity matches the aircraft's velocity as the satellite fixed in the sky.

4.6 Sub-model 4: Jamming link budget

Jamming relies on the deliberately weakening of the useful signal in relation to prevailing noise floor and interference. In situations where the jamming dominates over the natural noise sources, the relationship can be simplified to a signal-to-jamming ratio (SJR). In low jamming power scenarios, noise sources need to be also accounted for leading to the term of signal-to-noise+jamming ratio (SJNR) [43].

$$\text{SJR} = \frac{S}{J} \qquad \text{SJNR} = \frac{S}{J+N}$$

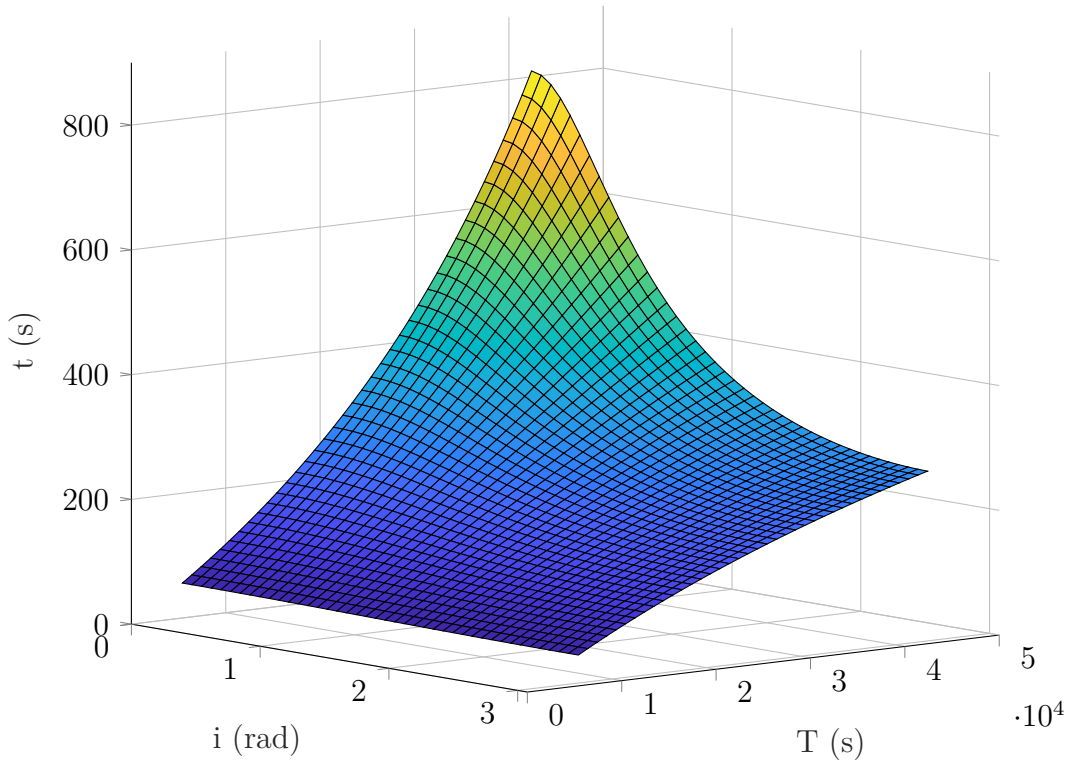

Figure 13: Listening window (s) as a function of orbital altitude (m) (korjaa metreiksi) and inclination (rad KORJAA ASTEET).

Transmission and jamming power levels S and J in decibel-watts (dBW) at the receiver can be calculated from the following equations.

$$S = P_t + G_{tr} - L_t - L_{tr}(R_{tr}) + G_{rt} - L_r \qquad \text{[dBW]} \tag{12}$$

$$J = P_j + G_{jr} - L_j - L_{jr}(R_{jr}) + G_{rj} - L_r \qquad \text{[dBW]} \tag{13}$$

In some cases, jammer may even be at an advantage based on their geographical location through a shorter signal path and smaller free space path loss, as demonstrated in [58]. Minimum CNR requirements for modulation and coding schemes (modcod) determine the ability of the jammer to interfere with the legitimate transmission. As discussed in chapter 2.1.3, OneWeb uses adaptive modcod scheme comprised of QPSK, 8PSK and 16-QAM modulation techniques. Higher end requires significantly greater CNR at the receiver, while the lower end can still function even with very low CNR, if significant forward error correction (FEC) is utilised. [26, 59]

Jamming of the uplink signal can be done from both aircraft and earth-bound platforms. Scenario-wise, the altitude of the interfering system does not make a major difference, if ground-level obstruction caused by structures and natural land formations is ignored. This simpified scenario allows E2E performance of a communications link can be analysed through a link budget, a theoretical calculation where gains and losses of a RF system are summed in order to compute a figures

of merit, such as x, y and z.Table 6 presents an uplink link budget for the Kymeta Hawk u8 UT interfacing with the OneWeb LEO megaconstellation. Parameters of the UT are taken from [60] and [61], while parameters for the space segment of the OneWeb constellation are based on the values in [23] and [26] for the first generation constellation. For the advantage of the legitimate user, the modcod scheme is assumed to be the less demanding QPSK with 1/2 FEC.

Satellite communication links are inherently long range in nature. When accounting for the losses in the RF path, this realisation allows for certain simplifications to be made without major losses in accuracy. RF path between the satellite and UT experiences losses primarily due to free space path loss (FSPL), a loss driven by the dispersion of RF energy into the medium it propagates through. FSPL in decibels can be computed from equation 14 based on the approximate orbital altitude satellites d in meters and UL frequency f in hertz.

$$\mathrm{FSPL} = 20\log(d) + 20\log(f) - 20\log(4\pi/c) \qquad [\mathrm{dB}] \tag{14}$$

In addition to FSPL, RF path may see varying losses from the athmospheric phenomena, such as rain or clouds or the athmosphere itself. It is worth noting, that the latter three tend to less significant when considering Ku and Ka-band propagation over signal paths ranging from hundreds to thousands of kilometers in space. This is due to FSPL growing to the square, while the other losses remain constant to a certain degree and tend to be magnitudes smaller.

Equation 12 was then simplified by summing the transmitter and jammer-related variables into the figure of effective isotropic radiated power (EIRP) with the satellite's receiver side boiled down to the figure of gain-to-noise-temperature (G/T). On the propagation side, both the legitimate transmitter and the jammer were assumed to be earth-bound and unobstructed. This allows the propagation losses to be estimated with the figures of FSPL and athmospheric loss. For the latter, a figure of 0.35 dB from [25] was applied. SNR was also normalised over 1 Hz of bandwidth.

$$S_{rx} = \mathrm{EIRP} - \mathrm{FSPL} - L_{ath} + \mathrm{G/T}_{sat} \qquad [\mathrm{dBW}] \tag{15}$$

The computations show that the jammer needs to achieve 1 dB smaller signal power at the satellite than the legitimate transmitter, meaning still a certain degree of advantage to the jammer at even the baseline scenario. Applying any of the more demanding modcod schemes, such as aforementioned 8PSK or 16-QAM, would push the SJR further to the jammer's benefit.

Jammer's capabilities are another point to consider. In principle, link budgets allow to examine the whole end-to-end RF chain. Despite this, analysis in table 6 was ended at the receiver of the satellite due to limited information available in the jammer's end. The spectrum of jamming devices varies from handheld ones all the way from high power vehicle or aircraft mounted systems. Most of the devices are highly classified military technology, exacerbating the issue of data scarcity even further.

Table 6: Uplink jamming link budget for Kymeta Hawk u8 flat panel terminal interfacing with the OneWeb LEO constellation.

Parameter	Value	Notes
Constants		
Athmospheric loss [dB]	0.35	
Bolzmann's constant [dBW/K/Hz]	-228.60	
Speed of light [m/s]	3.00E+08	
Satellite parameters		
Transponder bandwidth, RX [MHz]	120.00	
Path distance [km]	1,200.00	
G/T at satellite's RX [dB/K]	11.40	
Target SJNR [dB]	1.00	QPSK, 1/2 FEC
User terminal parameters		
Frequency [MHz]	14,000.00	
Broadside EIRP [dBW]	46.50	
Channel bandwidth [MHz]	20.00	
Computed values		
Free space path loss [dB]	176.95	
Channel bandwidth [dBHz]	73.01	
Received power @ sat [dB]	-192.41	
Required jamming power @ sat [dB]	-193.41	$J \gg N$

5 Discussion

Critical communication users demand robust solutions, particularly in terms of confidentiality, integrity, and availability. The historical limitations of satcom solutions, especially in the public safety sector, alongside the challenges faced by commercial systems, underscore the necessity for a nuanced understanding of these systems. With the increasing integration of satcom into both commercial and critical applications, the imperative to comprehend the underlying factors of these systems becomes paramount.

The primary focus involved applying quantitative analysis through the development of a robust threat model, targeting a Walker-type LEO megaconstellation, fixed Very Small Aperture Terminals (VSAT), and the influence of airborne eavesdroppers. The research framework comprised four smaller submodels, each explored through a parametric study, with a specific dependent variable and a set of independent ones. The foundation of the models rested on a first principles approach, employing geometric and kinematic analyses, as well as link budgets based on a representative hardware configuration. By deconstructing the target system into fundamental components, each submodel highlighted the potential strengths and vulnerabilities of satcom systems in relation to various threats.

As discussed in chapter 2.2, cruising speeds of aircraft are typically in the subsonic range. For example, at the operational altitude of an jetliner, this equates to roughly 900 km/h or 250 m/s. On the other hand, relative velocity of an satellite beam can vary wildy depending on the orbital altitude due to the varying angular velocity. Tracking potential of an airborne adversary was analysed in chapter 4.4 by computing the velocity of the passing beam at a range of typical aircraft altitudes. The computed values ranging from stationary at GEO altitudes to thousands of m/s for LEO satellites making the beam between an Earth-bound UT and a LEO satellite the hardest to track for an adversary due to the high angular velocity of the beam, and in turn resulting linear velocity at the full range of potential athmospheric cruising altitudes.

Legacy GEO systems may allow for an conveniently flying eavesdropper to intecept the UT's data stream endlessly, as the satellites remain in an inherently fixed position in the sky. In [62], the authors reckon that this vulnerability of GEO satellites is likely already exploited by space-borne inspection satellites, like the Luch-1 and Luch-2 of the Russian Aerospace Forces. These SIGINT satellites were launched in 2014 and 2022 and have been operating in proximity of western geostationary communications satellites over the years.

Similar to these sophisticated SIGINT satellites, an aerial platform may be able to eavesdrop geostationary satellites by loitering inside a beam for continued periods of time. We can use estimate the threat area of an individual aircraft based on its cruising altitude and UT's minimum elevation angle. Maximum range of an eavesdropper to listen to varies from hundreds of meters to over 100 kilometers depending on the aerial platform's capabilities and minimum elevation angle in the chosen satellite system. This means that the threat of an airborne adversary is generally quite localised, especially if the adversary is unable to operate in the airspace over of the target system's jurisdiction. More stealthier platforms like

balloons may though be able to evade tracking and with sufficien collusion extend the coverage inside the target country's borders.

Tracking potential ties also into the other concept analysed in chapter 4.5, the listening window.

One limitation of the link budget approach is that only part of the RF environment can be modelled with reasonable level of baseline assumptions. For example, jamming systems tend to vary greatly from handheld devices all the way from high power vehicle or aircraft mounted ones. Most of the devices are also highly classified military technology data availability being the key issue.

The computed link budget proves that that the jammer and legitimate user tend to be on rather equal footing with each other when it comes to basic service availability. The situation is though different, if we consider the requirements for higher QoS. Achieving higher throughputs necessiates the use of more complex modcod schemes that in turn require greater SNR or in our case SJR at the receiver's end. Here, the advantage can range from single to tens of decibels depending on the modulation utilised.

Similarly, the relative postion between the legitimate transmitter, satellite and jammer may present interesting opportunities to the jammer, where the link budget tips strongly in the interfering party's favour. On the other hand, the large number of LEO satellites in the megaconstellations leads to major redundancy in the choice of satellite. If a UT is configured wisely, it may be able to avoid jamming, especially if the latter is localised in nature, by just transmitting in the direction of the clear sky.

Tässä osassa esitetään tulokset ja vastataan tutkielman alussa esitettyihin tutkimuskysymyksiin. Tieteellisen kirjoitelman arvo mitataan tässä osassa esitettyjen tulosten perusteella.

Tutkimustuloksien merkitystä on aina syytä arvioida ja tarkastella kriittisesti. Joskus tarkastelu voi olla tässä osassa, mutta se voidaan myös jättää viimeiseen osaan, jolloin viimeisen osan nimeksi tulee »Tarkastelu». Tutkimustulosten merkitystä voi arvioida myös »Johtopäätökset»-otsikon alla viimeisessä osassa.

Tässä osassa on syytä myös arvioida tutkimustulosten luotettavuutta. Jos tutkimustulosten merkitystä arvioidaan »Tarkastelu»-osassa, voi luotettavuuden arviointi olla myös siellä.

6 Conclusion

In recent years, the satellite communications industry has witnessed a paradigm shift with the rise of large NGSO megaconstellations. The proliferation of these constellations, facilitated by reduced space launch costs and COTS technology, has opened new frontiers of connectivity. However, this rapid evolution has not been without challenges, particularly in the area of cybersecurity.

The absence of widely accepted cybersecurity standards and the proprietary nature of technical solutions leave open potential vulnerabilities, while the wide-area broadcast nature of satellite transmissions makes them susceptible to eavesdropping and other adversarial actions from a wide geographic footprint. Adversarial groups, including state actors and individual enthusiasts armed with accessible Software-Defined Radios (SDR), have demonstrated the feasibility of intercepting satellite traffic.

To better understand the underlying security aspects of emerging NGSO VSAT networks, this thesis focused on assessing the risks posed by airborne eavesdroppers to the uplink communications from satellite terminals on the ground. Through geometric and kinematic analysis, as well as link budgets based on typical hardware configurations, the resilience of LEO broadband systems was explored.

The unique attributes of the space environment, in which the satellite's space segment resides, give certain advantages to the LEO systems. Orbital motion of the satellites in LEO limits the listening window for communication interception, necessating large-scale collusion between eavesdroppers for effective COMINT. Additionally, the radio horizon arising from higher minimun elevation angles in VSATs imposes further constraints on eavesdroppers, requiring them to approach relatively close to transmitting terminals for effective uplink interception.

On the other hand, using lower orbits leads to certain disadvantages. While higher orbits like GEO require the eavesdropper to transmit at equivalent EIRP levels compared to the legitimate transmitter, the lower altitude of LEO introduces situations where jamming or hijacking the legitimate signal is possible to achieve even with relatively simple and inexpensive radio hardware, such as COTS SDRs and satellite TV equipment. Despite the relative ease of raw jamming, sophisticated spoofing attacks tend to be more difficult to achieve. Here, contributing factors are the complex and often obscure nature of satellite systems. It is worth noting that commercial broadband systems have been moving towards more standardised solutions in the recent years.

Public safety and defence users place more stringent requirements on their communication solutions when compared to commericial consumer and entreprise systems. Clear understanding of the control and ownership, as well as robust security measures, be they physical or cyber in nature, are the root prerequisites for the adoption of any new system or solution. Considering the results gained from the examination of the model, the emerging NGSO satellite networks do not have inherent physical flaws that would directly jeopardise the security of these systems. In fact and as discussed, compared to their predecessors, the NGSO systems have some inherent qualities that make them rather robust against a multitude of the potential threat factors.

Security of commercial satellite systems is a rather young field of study and much work remains for future researchers. Concerning the commercial broadband networks, approaches such as practical waveform studies through open-source black-box reverse engineering is one interesting approach. Robustness of physical and network security of the gateways is another interesting topic with less attention in the research literature.

References

[1] A. C. O'Connor *et al.*, "Economic benefits of the global positioning system (GPS)," 2019.

[2] V. Lupi and V. Morretta, *Socio-economic benefits of earth observation: Insights from firms in Italy*. OECD Publishing, 2022. [Online]. Available: https://www.oecd-ilibrary.org/content/component/5982c4af-en

[3] A. Tassa, "The socio-economic value of satellite earth observations: huge, yet to be measured," *Journal of Economic Policy Reform*, vol. 23, no. 1, pp. 34–48, 2020. doi: 10.1080/17487870.2019.1601565

[4] Euroconsult, "Space Economy Report," 2023, 9th edition.

[5] B. Lin, W. Henry, and R. Dill, "Defending Small Satellites from Malicious Cybersecurity Threats," in *International Conference on Cyber Warfare and Security*, vol. 17, no. 1, 2022, pp. 479–488. doi: 10.34190/iccws.17.1.60

[6] J. Pavur *et al.*, "A Tale of Sea and Sky On the Security of Maritime VSAT Communications," in *2020 IEEE Symposium on Security and Privacy (SP)*, 2020, pp. 1384–1400. doi: 10.1109/SP40000.2020.00056

[7] R. Santamarta, "A wake-up call for satcom security," IOActive, Tech. Rep., 2014. [Online]. Available: https://ioactive.com/a-wake-up-call-for-satcom-security/

[8] N. Boschetti, N. G. Gordon, and G. Falco, "Space cybersecurity lessons learned from the viasat cyberattack," in *ASCEND 2022*, 2022, p. 4380.

[9] N. N. Schia, I. Rødningen, and L. Gjesvik, "The subsea cable cut at Svalbard January 2022: What happened, what were the consequences, and how were they managed?" 2023. [Online]. Available: https://www.nupi.no/en/publications/cristin-pub/the-subsea-cable-cut-at-svalbard-january-2022-what-happened-what-were-the-consequences-and-how-were-they-managed

[10] M. Lee and E. Tucker, "US says China balloon could collect intelligence signals," Feb. 2023. [Online]. Available: https://apnews.com/article/chinese-balloon-military-involvement-e45c759cb00294e83989fa35970935bc

[11] J. M. Johansson and R. Grimes, "The great debate: security by obscurity," Microsoft Corporation, Tech. Rep., 2008-06.

[12] E. Diehl, *Law 3: No Security Through Obscurity*. Cham: Springer International Publishing, 2016, pp. 67–79. ISBN 978-3-319-42641-9

[13] W. Guo *et al.*, "Defending against adversarial samples without security through obscurity," in *2018 IEEE International Conference on Data Mining (ICDM)*. IEEE, 2018, pp. 137–146.

[14] N. Abdelsalam, S. Al-Kuwari, and A. Erbad, "Physical Layer Security in Satellite Communication: State-of-the-art and Open Problems," 2023, arXiv:2301.03672.

[15] I. del Portillo, B. G. Cameron, and E. F. Crawley, "A technical comparison of three low earth orbit satellite constellation systems to provide global broadband," *Acta Astronautica*, vol. 159, pp. 123–135, 2019. doi: 10.1016/j.actaastro.2019.03.040

[16] Euroconsult, "NGSO Constellation Tracker: Q3 2023 update," 2023.

[17] "IRIS² Industry Information Day: Annex II.A High Level Requirements – Main categories," Mar. 30 2023. [Online]. Available: https://defence-industry-space.ec.europa.eu/system/files/2023-03/IRIS2%20Industry%20Information%20Day%20-%2030%20March%202023.pdf

[18] NSR, "5G via Satellite, 4th edition – opportunities for satellite players," Oct. 2023.

[19] ——, "Satellite direct-to-device market," Sep. 2023.

[20] TeleGeography, "IP Networks Report: Executive Summary," 2023. [Online]. Available: https://www2.telegeography.com/hubfs/LP-Assets/Product-One-Pagers/product-page-content-samples/global-internet-geography/telegeography-global-internet-geography-executive-summary.pdf

[21] K. Çelikbilek *et al.*, "Survey on Optimization Methods for LEO-Satellite-Based Networks with Applications in Future Autonomous Transportation," *Sensors*, vol. 22, no. 4, 2022. doi: 10.3390/s22041421. [Online]. Available: https://www.mdpi.com/1424-8220/22/4/1421

[22] Y. Henri, *The OneWeb Satellite System*, J. N. Pelton, Ed. Cham: Springer International Publishing, 2020. ISBN 978-3-030-20707-6

[23] WorldVu Satellites Limited, "OneWeb K-band NGSO constellation FCC filing SAT-LOI-20160428-00041," Apr. 2016.

[24] M. S. Corson, "Admission control system for satellite-based internet access and transport," Dec. 10 2019, US Patent 10,506,437.

[25] "Link Budget Calculations for a Satellite Link with an Electronically Steerable Antenna Terminal," Jun. 1 2019, 793-00004-000-REV01.

[26] B. Allen, "Terrestrial meets non-terrestrial networks – a real-world example," 2022. [Online]. Available: https://www.cambridgewireless.co.uk/media/uploads/files/CWTEC22_-_Hybrid_-_Ben_Allen_OneWeb.pdf

[27] Space Exploration Holdings, LLC, "SpaceX K-band NGSO constellation FCC filing SAT-MOD-20200417-00037," Nov. 2016.

[28] N. Pachler *et al.*, "An updated comparison of four low earth orbit satellite constellation systems to provide global broadband," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2021, pp. 1–7. doi: 10.1109/ICCWorkshops50388.2021.9473799

[29] Space Exploration Holdings, LLC, "SpaceX K-band NGSO constellation FCC filing SAT-LOA-20161115-00118," Nov. 2016.

[30] A. Alamouri, A. Lampert, and M. Gerke, "An exploratory investigation of uas regulations in europe and the impact on effective use and economic potential," *Drones*, vol. 5, no. 3, 2021. doi: 10.3390/drones5030063. [Online]. Available: https://www.mdpi.com/2504-446X/5/3/63

[31] A. C. Watts, V. G. Ambrosia, and E. A. Hinkley, "Unmanned aircraft systems in remote sensing and scientific research: Classification and considerations of use," *Remote Sensing*, vol. 4, no. 6, pp. 1671–1692, 2012. doi: 10.3390/rs4061671. [Online]. Available: https://www.mdpi.com/2072-4292/4/6/1671

[32] "Joint Publication 3-30: Joint Air Operations," Jul. 25 2021. [Online]. Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_30.pdf

[33] M. Hassanalian and A. Abdelkefi, "Classifications, applications, and design challenges of drones: A review," *Progress in Aerospace Sciences*, vol. 91, pp. 99–131, 2017. doi: 10.1016/j.paerosci.2017.04.003

[34] M. H. Sadraey, *5. Straight-Level Flight - Jet Aircraft*. CRC Press, 2017. ISBN 978-1-4987-7655-4. [Online]. Available: https://app.knovel.com/hotlink/khtml/id:kt011MGRT3/aircraft-performance/straight-level-flight

[35] A. Filippone, "Data and performances of selected aircraft and rotorcraft," *Progress in Aerospace Sciences*, vol. 36, no. 8, pp. 629–654, 2000. doi: https://doi.org/10.1016/S0376-0421(00)00011-7. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0376042100000117

[36] E. B. Tomme and D. Phil, "The paradigm shift to effects-based space: Near-space as a combat space effects enabler," Airpower Research Institute, College of Aerospace Doctrine, Tech. Rep., 2005. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA434352.pdf

[37] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[38] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[39] A. D. Wyner, "The Wire-Tap Channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975. doi: 10.1002/j.1538-7305.1975.tb02040.x

[40] J. Barros and M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels," in *2006 IEEE International Symposium on Information Theory*, 2006, pp. 356–360. doi: 10.1109/ISIT.2006.261613

[41] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, 1978.

[42] "Joint Publication 2-0: Joint Intelligence," Oct. 22 2013. [Online]. Available: https://irp.fas.org/doddir/dod/jp2_0.pdf

[43] J. Kosola and T. Solante, *Digitaalinen taistelukenttä: informaatioajan sotakoneen tekniikka*. Finnish National Defence University, 2013. ISBN 978-951-25-2503-4

[44] N. R. C. et al., *Bulk Collection of Signals Intelligence: Technical Options*. National Academies Press, 2015. ISBN 978-0-309-32520-2

[45] "Joint Publication 3-85: Joint Electromagnetic Spectrum Operations," May 22 2020. [Online]. Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf

[46] M. Säynevirta, "Satellite Communications in Public Safety," Aug 2021, Airbus internal report.

[47] Erillisverkot, "Trump ja Putin tapasivat turvallisesti," 12 2018. [Online]. Available: https://www.erillisverkot.fi/trump-ja-putin-tapasivat-turvallisesti/

[48] TCCA, "Airbus' secure communications solutions deployed at Abu Dhabi Grand Prix 2021," 2021. [Online]. Available: https://tcca.info/airbus%E2%80%99-secure-communications-solutions-deployed-at-abu-dhabi-grand-prix-2021/

[49] Airbus Secure Land Communications, "Airbus supports F1 Bahrain Grand Prix 2023 with secure communication solutions," 3 2023. [Online]. Available: https://tcca.info/airbus%E2%80%99-secure-communications-solutions-deployed-at-abu-dhabi-grand-prix-2021/

[50] FirstNet Authority, "FirstNet - Helping Firefighters Face Historic Wildfire Season Amid Pandemic," Aug. 2021. [Online]. Available: https://www.firstnet.gov/newsroom/blog/firstnet-helping-firefighters-face-historic-wildfire-season-amid-pandemic

[51] ——, "FirstNet Authority Provides Update on Nashville Bombing ," Jan. 2021. [Online]. Available: https://www.firstnet.gov/newsroom/press-releases/firstnet-authority-provides-update-nashville-bombing

[52] M. Heikkilä *et al.*, "Field trial with tactical bubbles for mission critical communications," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 1, p. e4385, 2022. doi: https://doi.org/10.1002/ett.4385. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4385

[53] P. Järvinen, *Tutkimustyön metodeista.* Tampere: Opinpajan kirja, 2011.

[54] ——, *On research methods.* Tampere: Opinpajan kirja, 2004.

[55] S. T. March and G. F. Smith, "Design and natural science research on information technology," *Decision Support Systems*, vol. 15, no. 4, pp. 251–266, 1995. doi: https://doi.org/10.1016/0167-9236(94)00041-2. [Online]. Available: https://www.sciencedirect.com/science/article/pii/0167923694000412

[56] R. Wiley, *ELINT: The interception and analysis of radar signals.* Artech, 2006.

[57] J. S. Seybold, *Introduction to RF propagation.* John wiley & sons, 2005. ISBN 978-0-471-74368-2

[58] "DEF CON 30 – Dr. James Pavur – Space Jam: Exploring Radio Frequency Attacks in Outer Space," Aug. 2022. [Online]. Available: https://www.youtube.com/watch?v=Ouyln7CeWJU

[59] ETSI, "ETSI EN 302 307 V1.3.1: Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications (DVB-S2)," Nov. 2012.

[60] "Kymeta Hawk u8 Product Sheet," 2022, 700-00230-000 rev D.

[61] Space Exploration Holdings, LLC, "Kymeta 2nd gen u8 UT blanket authorisation FCC filing SES-MOD-INTR2020-01480," Jun. 2020.

[62] K. A. Bingen *et al.*, "Space Threat Assessment 2023," apr 2023. [Online]. Available: https://www.csis.org/analysis/space-threat-assessment-2023

A Appendix: Comparison of broadband satellite systems

Operator	Frequency band	Number of satellites, ph. 1 (launced / planned)	Number of satellites, ph. 2 (launced / planned)	Orbital altitude (km)	Latency (ms)	UT datarate	System throughput (Tbps)	Country of origin
Amazon Kuiper	Ka	0 / 548	0 / 3236	590-630		400 Mbps in tests		US
OneWeb	Ku, Ka	648 / 648	0 / 6372	1200	< 50 ms		10 Gbps	UK
SpaceX Starlink	Ku, Ka V, E, S	x / 4408	0 / 7518	$\sim$550 (ph. 1), $\sim$350 (ph. 2)	270-TODO	150 / 15 Mbps	$\sim$88 (ph. 1), $\sim$350 (ph. 2)	US
Telesat Lightspeed	Ka	0 / 298	0 / 1671	1015, 1325	700	7.5 Gbps UT, 20 Gbps "hotspot"		Canada
AST SpaceMobile	S, V	0 / 20	0 / 223	700	1500	35 / 3 Mbps		US
Lynk	S	0 / 5000		500	85			US
Iridium NEXT	L	75 / 66		780	680			US

B Appendix: Matlab code

KOODI TÄHÄN