Securing Uplink against Airborne Adversaries: A Security Analysis in Non-Geostationary Satellite Systems

Markus Säynevirta

School of Electrical Engineering

Thesis submitted for examination for the degree of Master of Science in Technology.
Espoo 29.12.2023

Supervisor

Assoc. 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 Securing Uplink against Airborne Adversaries: A Security Analysis in Non-Geostationary Satellite Systems

Degree programme Master's Programme in Automation and Electrical Engineering

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

Supervisor Assoc. Prof. Jaan Praks

Advisor M. Sc. (Tech) Tapio Savunen

Date 29.12.2023 **Number of pages** 60+4 **Language** English

Abstract

Since the late 2010s, the satellite communications industry has gone through a paradigm shift with the rise of large non-geostationary orbit (NGSO) megaconstellations. This shift, fuelled by reduced space launch costs and the widespread use of commercial off-the-shelf (COTS) technology, has ushered in a new era of broadband connectivity with truly ubiquitous availability of high-quality network access. Going forward, NGSO megaconstellations are likely to play a crucial role as a complementary solution for terrestrial mission-critical networks.

The rapid proliferation of commercial satellite solutions has not been without its challenges, particularly in the realm of cybersecurity. The absence of widely accepted cybersecurity standards, coupled with the proprietary nature of the technology, leave satellite systems open to potential vulnerabilities. Instances of interception and intentional interference have been demonstrated in the literature using readily available and affordable radio equipment, accessible even to hobbyists.

In this context, this thesis investigated the threat posed by airborne adversaries to the uplink communications of a very small aperture terminal (VSAT) interfacing with a megaconstellation in low Earth orbit (LEO). A research framework comprising four submodels was developed with the models examining VSAT interception range, beam tracking potential for airborne eavesdroppers, interception windows, and the active threat of jamming. Findings were examined from the perspective of mission-critical communications, and they proved the physical resilience of NGSO VSAT systems against signal interception and intentional jamming, with the distributed infrastructure of NGSO systems offering many inherent advantages. Therefore, commercial LEO megaconstellations offer new capabilities and enhance existing ones, even in the demanding fields of public safety and defence. However, their integration into critical communications infrastructure requires care due to the stringent cybersecurity requirements in these markets.

Keywords physical layer security, satellite security, critical communications, megaconstellations

Aalto University
School of Electrical
Engineering

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

Tekijä Markus Säynevirta

Työn nimi Uplinkin suojaaminen vihollisen ilma-aluksilta: turvallisuusanalyysi ei-geostationaarisista satelliittiverkoista

Koulutusohjelma Automaatio- ja sähkötekniikan maisteriohjelma

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

Työn valvoja Prof. Jaan Praks

Työn ohjaaja DI Tapio Savunen

Päivämäärä 29.12.2023 **Sivumäärä** 60+4 **Kieli** Englanti

Tiivistelmä

Satelliittiviestintä on mullistunut 2010-luvun lopulta alkaen uusien ei-geostationaarisia ratoja käyttävien megakonstellaatioiden yleistyessä. Laskevien laukaisukustannusten ja kaupallisen teknologian laajamittaisen käytön mahdollistamat megakonstellaatiot ovat avanneet uuden aikakauden laajakaistaviestinnässä tarjoamiensa maailmanlaajuisten ja suorituskykyisten palvelujen myötä. Kuluttajien ja bisneskäyttäjien ohella turvallisuuskriittiset toimijat, kuten viranomaiset ja maanpuolustusorganisaatiot, ovat osoittaneet kiinnostusta kaupallisten satelliittiverkkojen laajempaan käyttöön.

Kaupallisten satelliittipalveluiden nopea kasvu ei ole tapahtunut ilman ongelmia, etenkin, kun asiaa tarkastellaan tietoturvan kannalta. Standardoimattomat kyberturvallisuusratkaisut ja satelliittiverkkojen teknisten ratkaisujen suljettu luonne jättävät verkkoihin mahdollisia haavoittuvuuksia. Tutkimuksissa on löytynyt tilanteita, joissa puutteelliset tietoturvaratkaisut ovat jättäneet kaupalliset järjestelmät ainakin jossain määrin avoimiksi salakuuntelulle ja tarkoitukselliselle häirinnälle.

Tämä diplomityö pyrki arvioimaan ilmasta tapahtuvan salakuuntelun ja tarkoituksellisen häirinnän uhkaa hyvin pienen apertuurin päätelaitteen (engl. very small aperture terminal, VSAT) uplink-suunnan viestiliikenteelle, jota lähetetään päätelaitteelta matalalla Maan kiertoradalla lentävään megakonstellaatioon. Tutkimuskysymykseen pureuduttiin neljästä alamallista kootulla uhkamallilla, jossa tarkasteltiin radiotaajuista häirintää, ilma-aluksen saavutettavissa olevia sieppausetäisyyksiä ja -ikkunoita, sekä lentävän salakuuntelijan kykyä seurata VSAT-päätelaitteen kapeaa radiokeilaa. Mallin pohjalta tehtyjä havaintoja tarkasteltiin kriittisen viestinnän näkökulmasta. Tulokset osoittavat, että megakonstellaatioiden kanssa toimivat VSAT-päätelaitteet ovat oikein toteutettuna resilienttejä signaalin kuuntelua vastaan ja sietävät tahallista häirintää varsin hyvin konstellaatioiden hajautetun luonteen ansiosta. Kaupalliset matalan Maan kiertoradan megakonstellaatiot soveltuvat näin täydentämään turvallisuuskriittisen viestinnän kykyjä, joskin niiden integraatio vaatii edelleen riittävää huolellisuutta toimialan tiukoista tietoturvavaatimuksista johtuen.

Avainsanat fyysisen kerroksen turvallisuus, satelliittien tietoturva, kriittinen viestintä, megakonstellaatiot

Preface

I would like to express my sincere appreciation to both, my advisor, Tapio Savunen, and supervisor, Jaan Praks, who helped me navigate through the process of writing my thesis while working at Airbus Defence and Space during the latter part of my master's studies.

Looking back at my time at Aalto, there are several individuals to whom I owe gratitude for the enriching experiences of the past years. I want to especially acknowledge the Fjört boys and the community around Bikepoli, the cycling association at Aalto. Additionally, heartfelt thanks to some of my closest friends who have been with me since pre and primary school times. Thanks to all of you for making these years undoubtedly some of the most memorable ones.

Nice, 28.12.2023

Markus Säynevirta

Contents

Abbreviations

3GPP	3rd Generation Partnership Project
CNR	carrier-to-noise ratio
COMINT	communications intelligence
COTS	commercial off-the-shelf
DL	downlink
DoD	Department of Defense (U.S.)
EA	electronic attack
ECEF	Earth-centred – Earth-fixed
ECI	Earth-centred inertial
EIRP	effective isotropic radiated power
ELINT	electronic intelligence
EP	electromagnetic protection
ES	electromagnetic support
EU	European Union
FDMA	frequency division multiple access
FHSS	frequency hopping spread spectrum
FISINT	foreign instrumentation signals intelligence
FSPL	free-space path loss
G/T	gain-to-noise-temperature
GEO	geostationary Earth orbit
HALE	high altitude long endurance
IRIS^2	Infrastructure for Resilience, Interconnectivity and Security by Satellite
JP	joint publication
LASE	low altitude short endurance
LALE	low altitude long endurance
LEO	low Earth Orbit
LOS	line-of-sight
MALE	medium altitude long endurance
MTOM	maximum takeoff Mass
NDC	network data centre
NGSO	non-geostationary orbit
QAM	quadrature amplitude modulation
PoP	point-of-presence
RF	radio frequency
SIGINT	signals intelligence
SNP	satellite network portal
SNR	signal-to-noise ratio
TDMA	time division multiple access
UAS	unmanned aerial system
UL	uplink
UT	user terminal
VSAT	very small aperture terminal
VTOL	vertical takeoff and landing

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 [1], Earth observation [2, 3], and satellite communications [4, 5] has brought us ubiquitous connectivity in every corner of this world, while unlocking previously unimaginable capabilities in positioning, navigation, and timing, as well as intelligence, surveillance, and reconnaissance. Recently, the satellite communications industry has entered an era of rapid change. Since the early 2010s, the most prominent new trend has been the emergence of megaconstellations with hundreds to thousands of satellites in low Earth orbit (LEO). The raise of large constellations in non-geostationary orbits (NGSO) has been enabled by the falling cost of space launches and mass-production of satellite hardware based on COTS technology [5].

Aside from commercial markets, governmental organisations, such as civilian public safety authorities and defence ministries, are showing significant interest in the emerging commercial satellite communication solutions [6]. The transition of public safety organizations from narrowband to broadband terrestrial networks has highlighted commercial NGSO satellite systems as a promising option for establishing ubiquitous, low-latency broadband connectivity. This is particularly relevant in traditionally hard-to-serve areas, such as low-density rural regions with limited commercial potential for terrestrial mobile network operators. Government entities, placing a premium on the security and resilience of their communication solutions, are raising questions about the conformity of these systems to their stringent requirements. Therefore, demonstrating the robustness of commercial satellite systems against a growing number of cyber-capable adversaries is a prerequisite for their adoption in these market segments.

Despite their decades-long development history, current satellite systems still lack widely accepted cybersecurity standards [7], while technical solutions and their proprietary nature have 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 [8] where the feasibility of eavesdropping downlink (DL) satellite traffic was proven practically using widely available and 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. 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 only to the air interface of these commercial systems. Another third-party vulnerability assessment [9] uncovered serious design flaws in the implementation of satellite user terminal (UT) 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 [10] and the cable cut in one of the optical cables connecting the SvalSat ground station to mainland Norway [11]. 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 [12].

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 [7]. The validity of this approach has long been debated within research and industry circles [13], with the recent consensus being that security of a system should never rely exclusively on obscurity [14, 15].

Although much work has focused on long-standing geostationary Earth orbit (GEO) broadband and NGSO narrowband systems, as well as longer-term evolution of 5G and 6G non-terrestrial networks, little attention has been directed towards the security of emerging LEO broadband systems. Operators of the emerging systems tout their architecture-level resilience in their marketing, but academic literature on the topic is still rather scarce. Moreover, most of the research on satellite system protection has examined DL communication between the satellite and different Earth stations [16]. Furthermore, more capital-intensive space or airborne signals intelligence 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 address the gaps in understanding of the security aspects of this rapidly evolving technology.

This thesis assessed whether the presence of airborne eavesdroppers pose a risk to the uplink (UL) communications of emerging NGSO VSAT networks. To achieve this goal, a conceptual-analytical research approach was applied in the form of a threat model focusing on a Walker-type LEO megaconstellation, fixed VSATs and airborne eavesdroppers. The threat model consisted of four discrete submodels and explored the resilience of NGSO broadband systems through a parametric study. Here, a set of dependent variables of the submodels were the key to understanding the fundamental constraints of a NGSO megaconstellation from the perspective of VSAT UL communication with orbiting satellites with adversarial actions, such as deliberate eavesdropping and interference like jamming, being considered. To build a quantitative picture of the prevalent threat landscape, the analysis looked into geometric and kinematic factors, as well as radio frequency (RF) link budgets. Finally, the conceptual-analytical model was evaluated numerically against a set of known real-world system parameters and the findings were discussed in relation to the requirements set out 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 signal acquisition and detection for applications like RF geolocation or eavesdropping, as well as deliberate interference through RF jamming. Chapter 4 goes over the features of

the analytical submodels and presents the quantitative results from their numerical analysis. Chapter 5 discusses these findings and compares them against the end-user requirements set out in chapter 2. 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 an era of change. The most prominent new trend has been the emergence of megaconstellations with hundreds to thousands of satellites in NGSO. These systems have been enabled by the falling costs in space launches and the mass-production of satellite hardware based on COTS technology [4, 17, 18].

GEO satellites flying at 35 786 km 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 been estimated to bring roughly USD 70 billions of capital investment into the space during the deployment of their generation 1 and 2 constellations over the next two decades. Megaconstellations are a very capex heavy industry and broader economic pressures have led 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 pandemic. 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 connectivity, to large national and multinational projects like Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS^2) in the EU and the Guo Wang megaconstellation in China [4, 18].

In terms of maturity, SpaceX, OneWeb and SES O3b mPOWER are the farthest into the deployment with full global connectivity available as of December 2023. Amazon Kuiper and Telesat are still being developed, with service start expected for 2026 and 2027, respectively. SES O3b mPOWER operates in higher medium Earth orbit while the three others use LEO altitudes ranging between 200 to 2 000 kilometres. 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 VSATs [4, 18].

On the other hand, startups like Lynk and AST SpaceMobile are planning to deliver broadband service from orbit directly to unmodified 3rd Generation Partnership Project (3GPP) standardised 5G handsets. Support for the implementation of 5G non-terrestrial network standards defined by the 3GPP to the maximum extent

possible but following a gradual implementation approach is also a key requirement in the European IRIS^2 programme. All in all, 3GPP non-terrestrial 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 research and development 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 [19–21].

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 fully deployed capability of the first-generation NGSO systems [22]. Thus, satellite internet services are unlikely to completely replace terrestrial networks but will act as a complimentary coverage and capacity solution for both commercial and government user segments.

2.1.2 Key technical characteristics

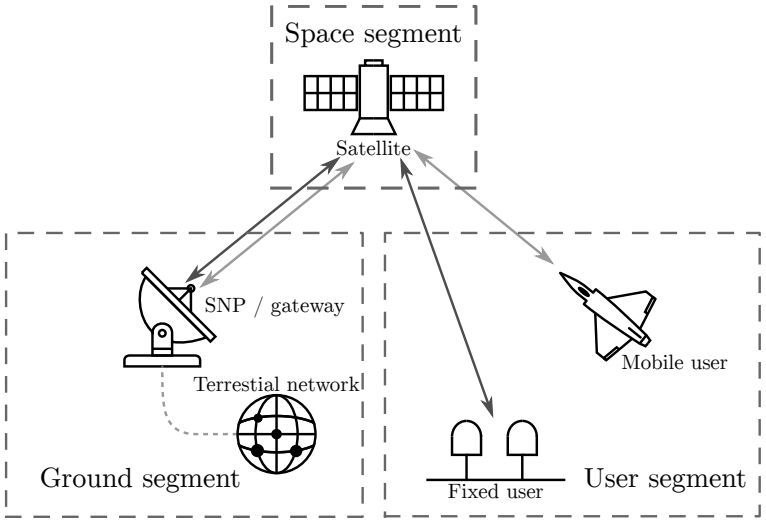

Figure 1: Typical high-level architecture of a satellite network. Differently shaded arrows between the segments correspond to individual data streams from the mobile and fixed users.

The design of a complete satellite system is a complex, multi-objective and multi-modal optimisation problem due to the inherently varying conditions and constraints in the ground, space, and user segments. Practically speaking, this requires tackling the overall optimisation problem segment-by-segment while considering the requirements of the target application. Figure 1 presents the three segments and interactions between them based on representations in [4] and [23].

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, directly affect the feasibility of user applications.

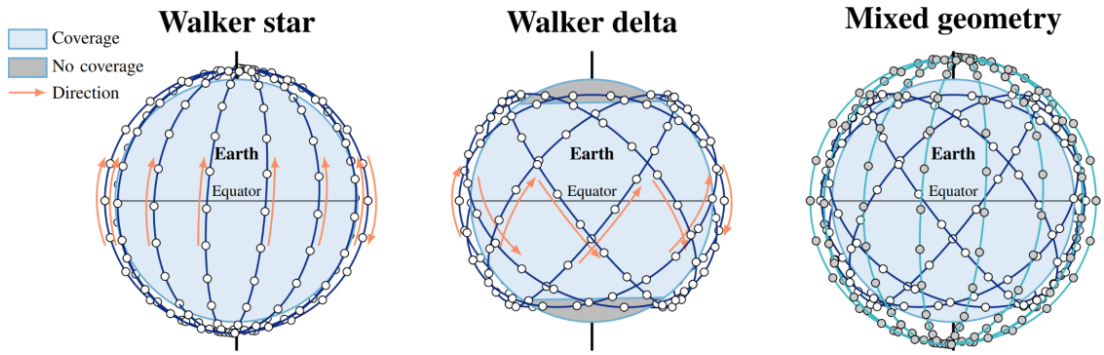

Figure 2: Three Walker constellation geometries: star, delta and hybrid combining the first two [24].

Walker constellations are a commonly used configuration for modern NGSO satellite systems thanks to its global coverage arising from the symmetrical distribution of satellites. Proposed originally in [25] and further developed in [26], Walker constellations consist of circular orbits described in terms of four design parameters: inclination i, number of satellites n, number of orbital planes p and relative spacing between satellites in adjacent planes f. The three latter parameters are often presented in the form $n/p/f$ when discussing different configurations. For example, Iridium's NGSO constellation could be described as a 66/6/2 Walker Star constellation with an inclination of 86.4 degrees.

Constellations can be further broken down into two main types based on the inclination: Walker Star constellations fly in near-polar orbits, covering the poles of the astronomical body, while Walker Delta constellations are lower-inclined, covering only lower latitudes of a body. Modern megaconstellations often consist of multiple Walker constellations at different altitudes and inclinations. In these hybrid configurations, a sub-constellation at a set altitude and inclination is typically called an orbital shell. The Starlink constellation is a fitting example of the latter, while Iridium and first-generation OneWeb are pure Walker Star constellations in terms of their orbital configuration. Figure 2 visualises the three constellation geometries.

Ground segment optimisation tends to be more straightforward. Ground station planning involves placing a number of stations in appropriate locations around the globe based on economic indicators such as overall deployment and ongoing maintenance costs of the ground station network, as well as more technical parameters like achieved sky coverage, system throughput and link capacity [23]. Finally, 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, [23] 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. In practice, NGSO megaconstellations are often built around vendor-specific UTs that relay the communications on dedicated Ka and Ku-band frequencies to the satellite constellation [4].

When it comes to LEO constellations, their altitude enables significantly lower latency, and the large number of satellites allows for high overall data throughput throughout a constellation when compared with the earlier satellite systems. Still, the most modern LEO megaconstellations fall short of the throughput of their terrestrial counterparts and are unlikely to completely replace the terrestrial mobile networks in their entirety. This has not put limits on the ambitions of the new market entrants. In fact, emerging NGSO operators are often promising to offer significantly 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, be it satellite or terrestrial in nature [4].

2.1.3 OneWeb system architecture

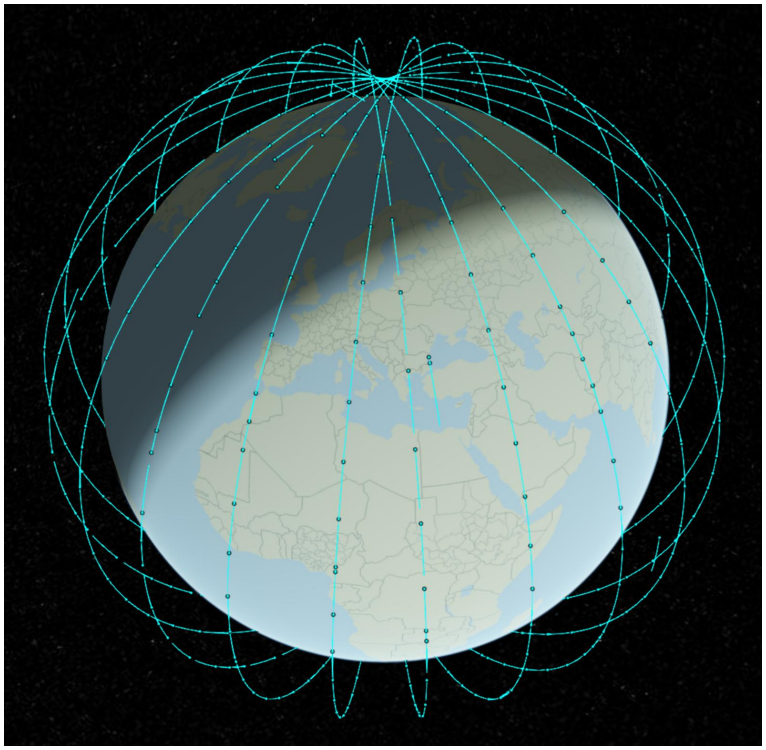

Figure 3: Simulation of the OneWeb system based on Celestrak TLE data from 11 December 2023.

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 several in-orbit spares. Operational satellites fly in an inclined polar orbit with an altitude 1200 km. Each satellite transmits and receives 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 [27, 28]. First-generation OneWeb satellites do not utilise inter-satellite links (ISL) [17].

Earth Stations of the OneWeb system can be broadly divided into three categories: tracking, telemetry, and control (TT&C) sites, gateways and 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 [28].

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 SNPs. 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 [27].

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 router. The latter connects the terminal to the end-user devices such as laptops or smartphones [27]. 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 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 [28].

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 radio access network, 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 base stations. 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 handovers in terrestrial networks [29].

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 [29]

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 UL and DL communications happen simultaneously in both forward and return links. For example, in the return direction, a UT uplinks to and the gateway DL from the satellite [30]. 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 [17, 28].

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 DL maps onto a predetermined Ka-band gateway UL and vice-versa in the return direction. [17, 28]

In the user link air interface, OneWeb uses a modified LTE waveform capable of adaptive modulation and coding. Different transmission schemes are employed depending on the link direction. In the forward direction, transmissions utilise time-division multiple access on a single 250 MHz wideband carrier (SC-TDMA) with each user terminal receiving the carrier and demodulating it, extracting relevant payload information based on the headers. Forward links employ turbo/convolutional/block channel coding and QPSK, 8PSK and 16QAM modulation [28, 31].

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 can access a single UL carrier based on time slots allocated by the network control centre. Terminals are also able to access multiple UL carriers based on the FDMA channel arrangement of the satellite in question. Like the forward link, return channel employs QPSK, 8PSK and 16QAM modulation but supports only turbo and block encoding [28, 31].

Generally speaking, Ka-band gateway-to-satellite links are asymmetric in nature. In terms of their channel configuration, the links employ 16 up and DL channels, bandwidth of individual channels being 155 MHz in the UL and 250 MHz in the DL direction. The links alternate between right and left-hand polarised (RHCP and LHCP) signals. Like 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 UL channels occupy 125 MHz of bandwidth while there are eight 250 MHz DL channels. Unlike the gateway links, the polarisation scheme of the signals is fixed based on the link direction, where UL utilises RHCP and DL is LHCP [17, 31].

Figure 4 visualises OneWeb's user link frequency band allocations in the Ku-band. User link structure is key information for the analytical portion of this thesis, and it is thus presented in more detail in figure 4. In the figure, UU denotes the transmission direction for uplink (UL), while UD indicates the direction for downlink (DL). The channel's placement on the upper right-hand (RH) or lower left-hand (LH) side signifies its polarisation, either right-hand or left-hand, respectively. Finally, the service type of the channel is denoted by the three-letter acronym above its band. FSS refers to fixed satellite services while TMS and TFS denote terrestrial fixed and terrestrial mobile services, respectively.

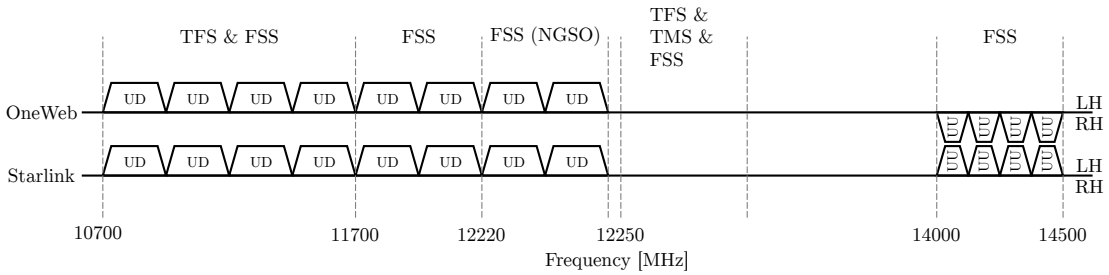

Figure 4: User link frequency band allocations of OneWeb and Starlink in the Ku-band [17].

2.1.4 Starlink system architecture

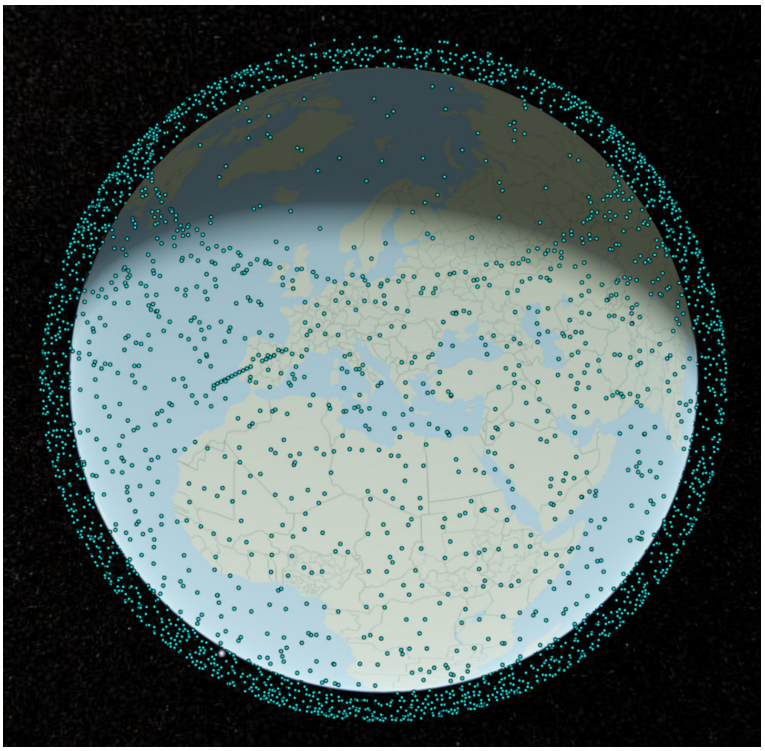

Figure 5: Simulation of the Starlink constellation based on Celestrak TLE data from 11 December 2023.

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 [32, 33].

First-generation Starlink satellites communicate with UTs through Ku-band links at a minimum elevation angle of 25 degrees. In the space segment, traffic is either

Table 1: Orbital shells and planes of the Starlink constellation [32].

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

relayed to other satellites via optical ISL or to gateways on higher frequency Ka-band links. Satellites have four phased array antennas, three of which function as DL and one as UL. All four arrays are capable of projecting eight independently shapeable and steerable spot beams, resulting in a 3-to-1 DL-to-UL ratio. Gain contours for both Ku and Ka-band beams are dependent on the steering angle, with values farther from boresight making the beam footprint more elliptical. Overall beamwidth is controlled by selectively switching on additional phased array elements as the steering angle gets farther from nadir. Depending on the steering angle, a spot beam can cover a range of individual cells, which are arranged based on Uber's H3 hexagonal cell system. Each spot beam covers roughly one size 5 hex cell at nadir [32, 34].

SpaceX has released limited details on the modulation and coding used in Starlink UL and DL communications. In [35], the researchers were able to reverse engineer the Starlink waveform to evaluate its usefulness in positioning, navigation, and timing applications. They found that the DL signal of a Starlink satellite is orthogonal frequency-division multiplexing. Empirical signal captures showed that the symbols in a Starlink DL transmission use quadrature amplitude modulation with 4- and 16-point constellations (4-QAM and 16-QAM). This aligns with SpaceX FCC filings, such as [36] concerning blanket-authorised terminals and in-flight connectivity, stating that the UTs support modulation schemes up to 64-QAM on both Ku-band UL and DL. Starlink's user link frequency allocations in the Ku-band are presented along OneWeb's in figure 4.

Like OneWeb, Starlink's ground segment comprises of both UTs and gateways and their associated network infrastructure, such as PoPs and NDCs. Starlink's Ka-band 1.5 m gateway antennas are globally distributed and arranged in clusters of nine antennas per site. When it comes to UTs, Starlink's lineup is simpler thanks to the SpaceX's vertically integrated terminal strategy. Half-power beamwidth of first-generation Starlink terminals varies between 2.8 and 5.5 degrees depending on the beam steering angle and whether the terminal is receiving or sending. Beamwidth figures are smaller for transmission and angles closer to boresight [36]. As of December 2023, SpaceX's terminal lineup includes two fixed flat panel terminals and two actuated ones. Size varies from smaller consumer terminals at an array size of 303 mm by 513 mm to larger high-performance variants at 575 mm by 511 mm [37].

2.2 Classification of aerial platforms

Aerial platforms have a long history in reconnaissance applications, going back all the way to the use of observation balloons in the battle of Fleurus in the late 18th century [38]. Modern platforms have come a long way from these primitive systems reliant on the human eye for surveillance in terms of sensing capability, manoeuvrability, and performance. Nowadays, mainstream aerial surveillance platforms range all the way from COTS multirotor drones to manned electronic warfare and signal intelligence capable jet aircraft in the tens of tonnes of dry mass. Understanding the defining physical features and potential limitations of these platforms is a key stage in evaluating their threat to VSAT satellite systems.

Aerial platforms can be categorised in a multitude 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 seen for example in the drone regulation of the European Union Aviation Safety Agency. The framework in the 2020 regulation splits unmanned aerial systems (UAS) into three distinct operational categories, which are open, specific, and certified. The risk model considers four core factors in its evaluation: maximum take-off mass (MTOM) of the UAS, whether the payload is hazardous, whether the vehicle is flown in visual line-of-sight (LOS) of the operator and at what altitude [39].

Risk-based approaches tend to be primarily mass-driven. Thus, to gain a more holistic picture of the platform under evaluation, we may want to introduce some additional factors into the classification. While there is an almost endless list of potential variables to classify a complex system, the top-level categories of performance, payload, system configuration tend to encompass the most relevant for different aerial platforms, be they a heavier manned aircraft, lighter-than-air craft or fixed or rotary wing UAS. Figure 6 visualises the classification originally devised by the U.S. Department of Homeland Security in terms of operational altitude and endurance.

In [40], the authors looked at classifying variety of UAS and potential 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 and landing craft (VTOL), low altitude short endurance (LASE) UAS, close proximity LASE (LASE Close) UAS, as well as low, medium, and high-altitude long endurance UAS (LALE, MALE and HALE). Figure 6 presents the prior categories in terms of MTOM and operational altitude with LASE and LASE Close combined into a single category.

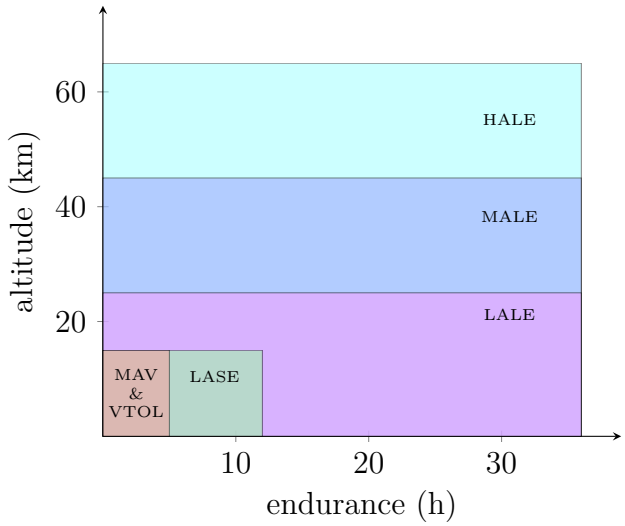

Figure 6: UAS classification in terms of operational altitude (kilometres) and endurance (hours) [40].

It is worth noting, that the U.S. Department of Defense (DoD) switched to a joint classification scheme for UAS in early 2010s. As described in [41], 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 groups as they are defined in [41]. The imperial units of the original classification have been converted to metric and rounded for the sake of readability.

In [42], the authors propose a more fine-grained classification. While the classification is detailed in terms of different structural sub-types, the basic approach is still like the previous classification models following a mass-and-size-based approach. On the highest level, their classification breaks UAS into six categories: normal and small UASs, and micro-, nano- and pico air vehicles denoted by UAV, µUAV, MAV, NAV, PAV, while SD refers to the so-called smart dust, the smallest air vehicle type currently in existence. The mass-and-size top-level classification is complemented by a more fine-grained one based on structural configuration. Figure 7 presents the classification in more detail. Third-level categories of rotary wing and Bio nano and micro air vehicle 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 manoeuvres. 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 behaviour during the cruise phase. Given the dominance of cruising flight over the

Table 2: UAS classification groups of the U.S. DoD [41].

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

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 [43].

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. Like the aforementioned classification frameworks for UAS, manned aircraft can be categorized through several parameters. In [44], the authors propose a 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 metrics such as wingspan, 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

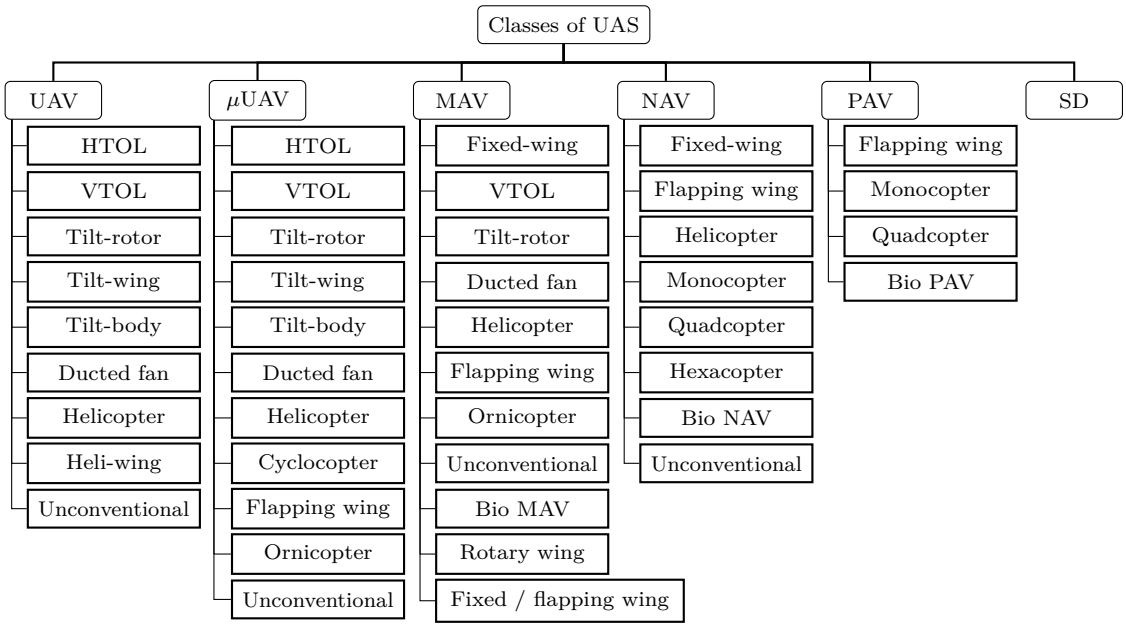

Figure 7: An UAS classification scheme derived from [42].

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.

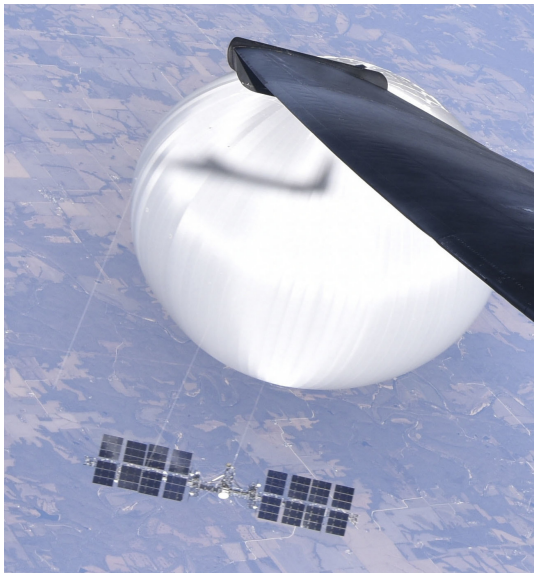

Figure 8: Chinese surveillance balloon over the Central United States as photographed from a U.S. Air Force U-2 on February 3. High-altitude balloons have potential for aerial signals intelligence due to their low radar cross section and the wide area of coverage arising from their stratospheric cruising altitude [45].

High-altitude balloons are also an interesting platform type when considering

their applicability for signals intelligence. These systems are interesting due to their low radar cross section and HALE capabilities enabling in turn a relatively wide area of coverage [45]. Figure 8 shows the Chinese surveillance balloon flying over the Continental United States as photographed from a U.S. Air Force U-2 during a widely reported incident in early 2023.

The goal of the analytical 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 manoeuvrability, the latter being especially interesting, as it can greatly vary between platform types. For example, lighter than air aircraft, such as high-altitude balloons have relatively limited manoeuvrability, as they rely on atmospheric air currents to carry them around.

The analytical section of this thesis aims to evaluate the vulnerability of VSATs to airborne adversaries by considering critical factors that define an aircraft's performance. These factors include cruising speed, altitude, payload mass, endurance, and, notably, manoeuvrability. The latter aspect is particularly intriguing due to its significant variation among different platform types. For instance, lighter-than-air aircraft, like high-altitude balloons, demonstrate limited manoeuvrability as they depend on atmospheric air currents to propel them around. In contrast, modern jet aircraft have great endurance and carry vast payloads but have typically larger radar cross section and are generally more resource-intensive to operate. Although not considered within the scope of this thesis, this presents and interesting optimisation problem for the adversary.

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 [46]. This core principle of secure communications was formalised by Shannon [47] 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 rarely to real-world systems, where some noise is always present [46].

Wyner [48] 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*. 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 [49]. 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 [46].

Wyner's degraded wiretap channel model is not entirely satisfactory as it assumes the eavesdropper to be at a disadvantage to the legitimate user. To address this issue, Csiszár and Körner [50] developed a more general approach that they termed the *broadcast channel with confidential messages*. The model involves two receivers and a sender transmitting two messages at the same time. The first message, a common one, which is intended for both receivers, is meant for both receivers, while the second, an individual secret message, is only for the intended receiver, treating the other receiver as an eavesdropper. If the second message is only transmitted, the channel is called a *wiretap channel* [46].

These seminal works form the foundation for physical layer security research. Analytical portion of the thesis will examine security of communications channels in the context of NGSO VSAT networks, bridging the theoretical underpinnings with real-world considerations. As we delve into the analytical portion of the thesis, we aim to apply and extend these foundational ideas to the specific challenges of NGSO VSAT networks. By examining the security of communications channels in a practical, applied setting, we seek to elucidate the real-world implications of these seminal theories and contribute to the evolving field of physical layer security in satellite communication systems.

2.3.2 Signals intelligence: ELINT, COMINT and FISINT

U.S. 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. JPs establish foundational doctrinal framework, ensuring standardized procedures for planning, executing, and evaluating military operations, playing an integral role in facilitating a collective understanding and helping synchronise 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 [51], 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) analyses 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 [52], FISINT is often grouped together with ELINT, if the latter is discussed in the broader non-communications context. Similar thinking is echoed in [53].

Considering satellite communication systems, the two disciplines of signals intelligence provide a wide range of tools for intelligence gathering at various 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 and radiopositioning may still yield valuable insights into the nature of the utilized systems, the user organisations, use patterns.

2.3.3 Electronic warfare: attack, protection, and support

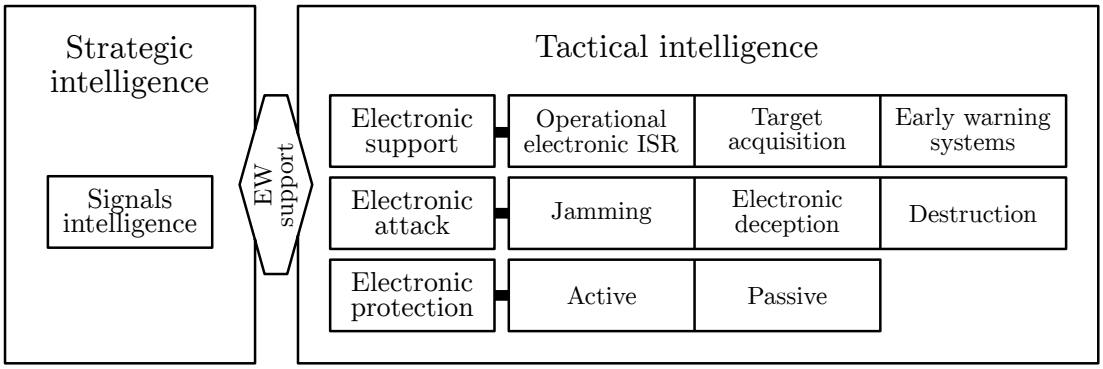

Figure 9: Electronic warfare taxonomy based on [52].

Electronic warfare involves military actions leveraging electromagnetic and directed energy to either control the electromagnetic spectrum or to launch attacks against the enemy. This multifaceted domain comprises three distinct divisions: electronic attack (EA), electromagnetic support (ES), and electromagnetic protection (EP) [52, 54].

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. Notwithstanding 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 [54], "it can be said that information collected from the [electromagnetic spectrum] has “two lives.” The first is as ES, unprocessed information used by operational forces to develop and maintain [situational awareness] for an

operationally defined period. The second is as SIGINT, retained and processed under appropriate intelligence authorities in response to specified intelligence requirements."

EA constitutes another key facet of electronic warfare, 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. EP, the third division, 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 involves direct action against an adversary via methods like jamming and spoofing. EP on the other hand is not concerned with directly affecting a target system or gaining information from it, but rather protecting friendly systems from external electromagnetic threats [52, 54].

2.4 Critical communications

2.4.1 Use cases and scenarios

Critical communications service operators tend to 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 [55].

Permanent applications tend to be the most obvious when it comes to the typical locations. They encompass the traditionally difficult-to-serve regions. For example, sparsely 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 [56–58]. 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 [59, 60].

Another distinguishing factor among the aforementioned events lies in their predictability and typical duration. Both planned and unplanned occurrences can

extend from days to months, influencing the selection of the most appropriate technological solution. The distinction between planned and unplanned events is not straightforward; rather, these concepts exist on a spectrum of various shades of grey. For instance, natural disasters like earthquakes can inflict unforeseen damage, necessitating an immediate response. Conversely, certain weather events, such as hurricanes and forest fires, may exhibit varying degrees of predictability. On the other hand, permanent satellite connectivity is the best suited to backhaul applications in extremely remote locations where constructing terrestrial networks proves to be impractical.

In summary, satellite connectivity acts as a complement to traditional terrestrial networks rather than a replacement, primarily due to the limited load-carrying capacity in terms of total and per-satellite throughput. Importantly, this limitation is generally not problematic in lower user density geographies, which are the primary areas for their utilisation. Therefore, once deployed in their first-generation configuration, broadband satellite systems provide a cost-efficient solution for filling gaps in global mobile connectivity, whether they are permanent or temporary in nature.

2.4.2 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 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 [61].

In the case of public safety communications, this leads to high requirements for availability even in a state of emergency. Like more traditional terrestrial networks, 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 the best suited to supporting response efforts 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 even most nation-states to implement. This is due to the immense capital requirements, especially when considering LEO options, which require a minimum of 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. 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 context of EU member states, the latter is probably the most attractive option, especially from the perspective of critical communications users. 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 [62].

Cost considerations are also crucial in this discussion, given that they have historically hindered the widespread adoption of existing satellite services. The success of the new constellations hinges on achieving significantly lower per-user costs, a vital factor for gaining broad acceptance. In the context of the public safety sector, it is important to note that this sector, particularly for smaller countries like Finland, is considered a niche market in the eyes of constellation operators. Consequently, achieving wider adoption in commercial markets becomes crucial in order to realize the economies of scale necessary for cost-competitive solutions that align with the limited budgets of public safety organizations. In practice, 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 when it comes to niche segments like public safety. In this senses, 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, like Erillisverkot in Finland or BDBOS in Germany [55].

Straightforward usability of the systems is crucial 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 tightly integrated with the existing communications infrastructure for it to be effective, so that it can be used when necessary.

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 push-to-talk, 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. This may require special arrangements in timing critical applications, as satellite systems

have longer end-to-end delay times compared to terrestrial systems. 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 [55].

2.4.3 NGSO connectivity in the 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 Critical Communications Broadband Group 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 Virve 2 in Finland, Réséau Radio du Futur in France, and Emergency Services Network in the United Kingdom [63].

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 so-called MCX services, where the X stands for mission-critical services like push-to-talk (i.e. voice), data, video. At the same time, reliable access to magnitudes greater bandwidth is crucial to enable nonstop access the full suite of mission-critical services. 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 [55].

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 [55].

When it comes to integration of satellite communications for critical communications use cases, permanent ones tend to be the most straight forward. They can be realised just as a simple fixed backhaul link of an individual base station site with currently available COTS satellite equipment. On the other hand, direct satellite connectivity is also something that may be feasible in these regions long-term, but its technological maturity remains low at the time of writing.

Implementation-wise, satellite networks are in the short-to-medium term envisioned to integrate into their terrestrial counterparts through portable tactical bubbles, where the satellite link serves as a backhaul solution for a local, 100 meters to kilometres in radius, wireless connectivity bubble. Table 3 lists technical and

functional requirements relevant for dimensioning a backhaul link for a 4G tactical bubble. Considering these requirements as well as form-factor and cost of COTS satellite equipment, best deployment model for integration of satellite services in mission-critical contexts seems to be a vehicular solution, an approach that is already seen to some extent in the ongoing migration projects. For example, in the future French broadband network, satellites are included as one backhaul option for a vehicular relay (*relais véhiculaire*), an emergency vehicle with a tactical bubble for local coverage and capacity. Similarly, the potential integration point for satellite systems in the Finnish Virve 2 has been envisioned as a command vehicle of fire, rescue, and police forces, but the solution is in the Finnish case on an early conceptual stage [55, 64, 65].

Long-term, evolution towards direct-to-smartphone type solutions is a potential development path. 3GPP has been working towards integrating satellites as one of the connectivity options in the 5G non-terrestrial networks, a development item also present on the longer reaching 5G Advanced and 6G roadmaps [66, 67]. The technological maturity of integrating satellites into existing mobile networks is still relatively low. While some solutions have been demonstrated in orbit, they have not yet entered commercial markets as of December 2023 [68–71].

Table 3: Technical and functional requirements for tactical bubbles [72].

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.)	DL / user	50 Mbps
	UL / 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 (UAS)	Latency	40 ms to 1 s

3 Research material and methods

3.1 Research questions and methodology

Critical communications users have a high standard for the communications solutions that they utilise. Less-capable narrowband NGSO and higher-latency GEO solutions have seen previously limited use in the public safety sector. Commercial systems have also turned out to be not the most robust when it comes to fundamental concepts of security, such as confidentiality, integrity, and availability, with critical vulnerabilities reported regularly in research literature over the years [7–9, 11]. With the recent drive to integrate satellite communications into both commercial and mission-critical communications solutions, satellite systems need to be able to prove that they can overcome these previous challenges. Here, understanding these systems from first principles is a good starting point for building a solid foundation for applied security research over factors like encryption, authorisation, and authentication.

The thesis seeks to answer whether airborne eavesdroppers and jammers can interfere with or intercept and decode UL communications in NGSO VSAT networks. 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 SIGINT. Threat model builds upon theory discussed in [52] and [73]. Target systems are explored through a parametric study of an analytical model comprised of multiple submodels that incorporate relevant parameters for aerial SIGINT platforms and both space and ground segments of a satellite communications system.

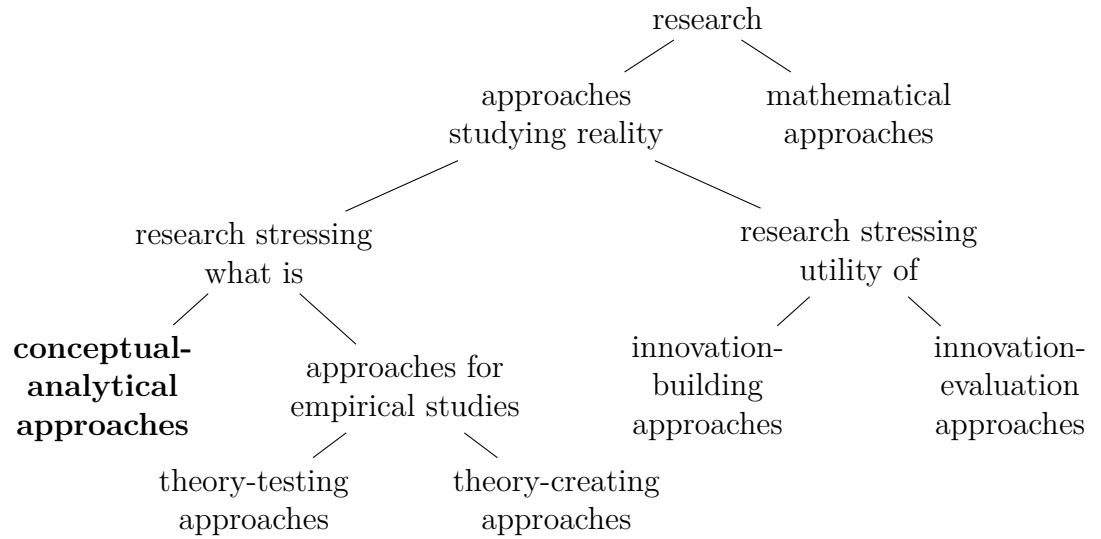

Figure 10: Research approach taxonomy of Järvinen [74, 75]. Conceptual-analytical approach followed in this thesis is highlighted.

Järvinen [74, 75] offers a comprehensive framework for categorizing research approaches, building upon the foundation laid by March and Smith [76]. Within this taxonomy, this thesis falls under the conceptual-analytical research approach, the scope being technology-oriented in nature. The other five research approaches of

the taxonomy are mathematical, 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). On the other hand, conceptual-analytical 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. The taxonomy proposed by Järvinen in [74, 75] is presented in figure 10.

3.2 Threat model

The core goal of this thesis is to assess whether the presence of airborne eavesdroppers poses a risk to the UL 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 several 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.

For the adversary to interfere with or eavesdrop on a legitimate transmitter, it must receive a sufficiently strong RF signal from the transmitter or be able to drown it out at the satellite's receiver. The former is the case when intercepting and decoding a signal, and the latter when attempting to jam or spoof the legitimate user. This scenario was systematically examined 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 vulnerabilities of satellite systems through an elemental understanding of the underlying physical phenomena.

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 narrow beam pattern of a few degrees of half-power beamwidth. Relative motion between the beam and an intercepting aircraft is a

Table 4: Descriptions for the submodels.

submodel	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

major consideration when it comes to evaluating the vulnerability of different satellite systems. Submodel 4 examines a jammer's ability to interfere with a legitimate UT interfacing with a LEO megaconstellation. Link budget for an UL 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 submodels.

submodel	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 Results

4.1 Submodel 1: Maximum interception range

To successfully eavesdrop on a target transmitter, an eavesdropper must intercept a sufficiently strong UL 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 gives a rise to two situations 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, both existing and under development broadband VSAT systems 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 general rule. In terms of frequencies, both bands fall under super high (3–30 GHz) to extremely high frequencies (30–300 GHz), where the principal propagation mode is LOS propagation. In LOS propagation, the radio horizon of a transmitter can be derived from the trigonometric law of cosines, if the planetary body can be assumed to be spherical in shape. If the minimum elevation angle of the satellite system is assumed to be zero, the geometry of the problem simplifies into a right triangle, whose hypotenuse and legs are described by the Pythagorean theorem.

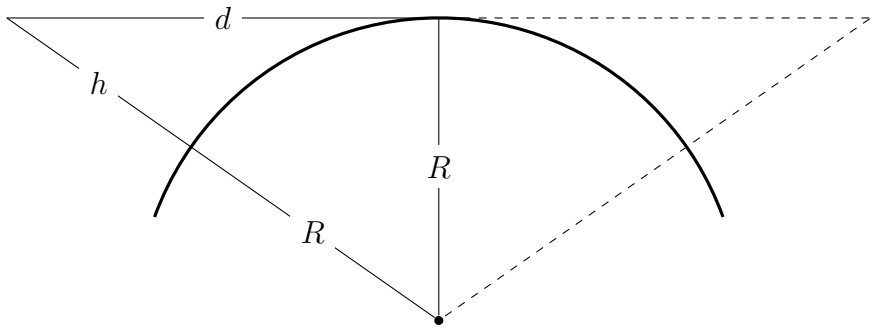

Figure 11: Geometry of ideal LOS propagation over a circular body [77] when the minimum elevation angle e is assumed to be zero.

In the simplified right triangle scenario, LOS distance d between the VSAT and the airborne eavesdropper forms one leg of a right triangle with the radius of the body R being the other one. This leaves the hypotenuse, which is in this case the transmitter's distance from the centre of the body $(R + h)$ [77]. The relationship between the quantities is visualised in figure 11. Equation 1 shows the mathematical relationship of these quantities in the form of the Pythagorean theorem.

$$d^2 = (R + h)^2 - R^2 = 2R \cdot h + h^2 \tag{1}$$

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

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

It is worth noting that equation (2) applies only in vacuum. Vertical pressure variation of an atmosphere 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 (2). In case of the Earth, an effective radius of 4/3 is usually applied [77].

$$d \approx \sqrt{2k \cdot R \cdot h} \tag{3}$$

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 the highly directional beam of a VSAT, thus requiring additional factors to be considered. Here, one of the most important parameters is the minimum elevation angle of the satellite system in question. Like radio horizon, maximum VSAT interception range can be examined through a trigonometric approximation model. Typical minimum elevation angles range from 20 to 55 degrees in modern LEO megaconstellations, as shown in appendix A. In this case, a more accurate interception range estimate can be computed based on the rule of cosines, where the model also accounts for the curvature of the body.

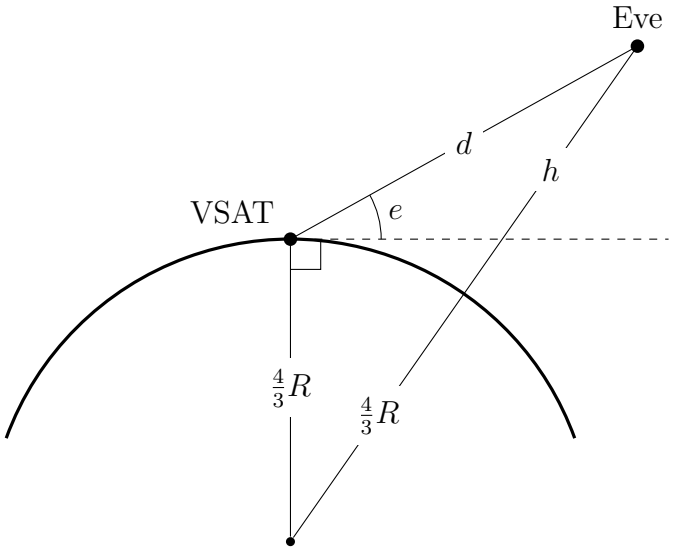

Figure 12: Rule of cosines.

If the operational altitude of the eavesdropper is known, theoretical maximum interception range can be computed for a range of the minimum elevation angles by

using the law of cosines. Rearranging for interception range d results in a complete quadratic equation, from which d can be solved by discarding the negative roots. Geometrically, the measurands form an obtuse triangle with the acute angle θ formed by d and R opposite to $h + R$ the distance of the airborne eavesdropper from the centre of the body. As minimum elevation angle e is measured from tangent of the body's radius, the acute angle θ is the sum of e with 90 degrees. Figure 12 visualises the geometry of this scenario.

$$h + r = \sqrt{d^2 + r^2 - 2dr\cos(e)} \tag{4}$$

As discussed, the purely trigonometric approach applies only in vacuum conditions. In the case of the Earth, curving of a RF signal in the atmosphere can be accounted for by using the 4/3 multiplier for the radius. Combining these factors and solving for intercept range d gives two equations, one of which can be discarded due to it giving negative range results. Thus, we end up with the following equation:

$$d = \frac{1}{2}(\sqrt{4h(h + 2r) + 4r^2\cos^2(e)} + 2r\cos(e)) \tag{5}$$

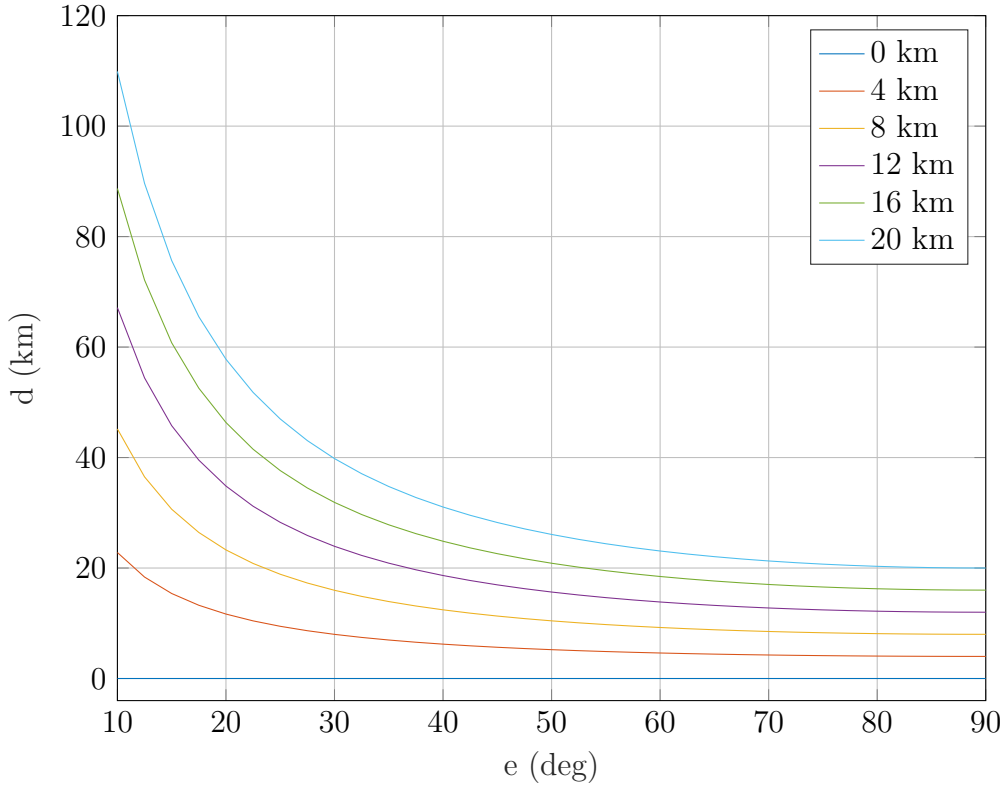

Figure 13: Interception range (d) as a function of minimum elevation angle (e). Different coloured graphs represent a range of operational altitude of the eavesdropper (h).

Figure 13 shows the interception range d as a function of minimum elevation angles $e = [0°, 90°]$. Values of e were plotted for six operational altitudes ranging between $h = [0, 20]$ kilometres. Independent variables e is on the horizontal axis, while the dependent variable d is on the vertical axis and has been calculated for a number of h values.

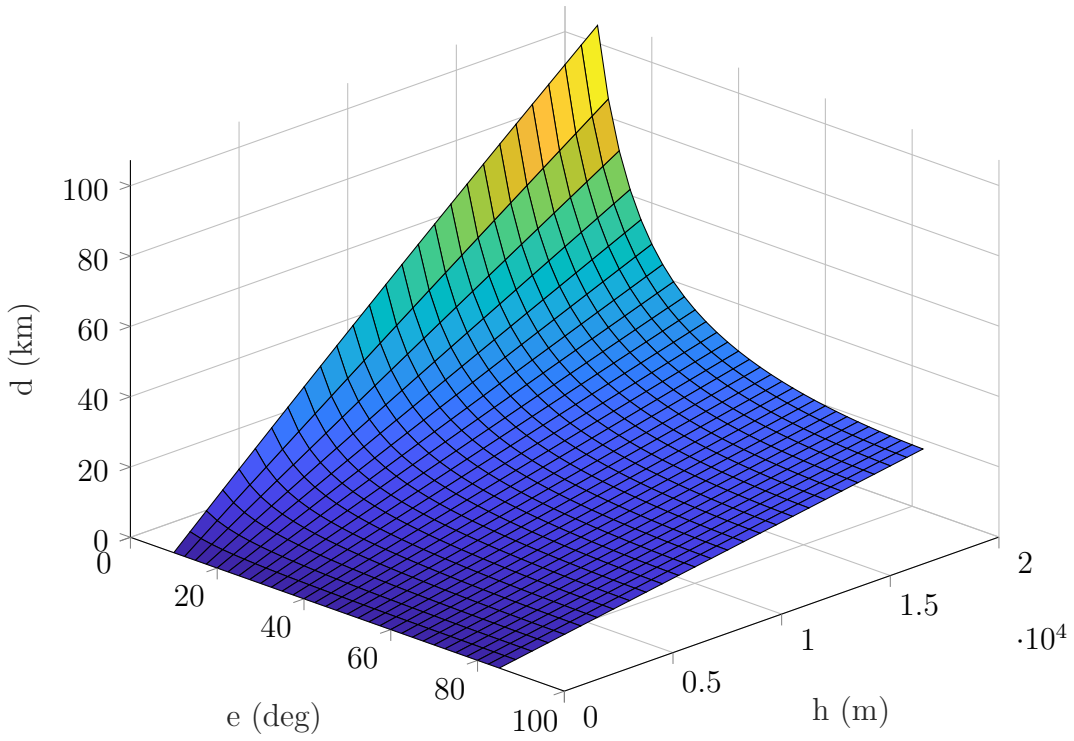

Figure 14: Interception range (d) as a function of minimum elevation angle (e) and operational altitude of the eavesdropper (h).

Figure 14 shows a three-dimensional representation of the same relationship within the limits $e = [10°, 85°], h_{Eve} = [100, 20000]$. In the resulting 3D plot, the dependent variable d is on the vertical axis while independent variables e and h form the horizontal axes.

The convex surface shows linear growth in relation to altitude h and accelerating tangential growth in relation to e. 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 on d is markedly smaller but still significant, especially when considering terminals with small e.

Although not applied in the analytical work in the thesis, the problem may be still simplified further if the curvature of the body can be ignored, a typical situation when it comes to LOS propagation at short ranges of tens of kilometres. In this further simplified scenario, the trigonometric tangent function of the interception range triangle can be written as

$$\tan(e) = \frac{h}{d} \tag{6}$$

where e is the minimum elevation angle of the user terminal, h is the operational altitude of the intercepting airborne platform and d is its distance from Alice on the ground, in essence the interception range. Rearranging (6) for d gives

$$d = \frac{h}{\tan(e)} \tag{7}$$

Although approximate in its results, this simplification may be used to gain quick insight into the threat of an eavesdropper operating at close ranges.

Based on the interception range estimations, we can say that eavesdropping a VSAT interfacing with a NGSO megaconstellation is a difficult endeavour, as was postulated in the hypothesis of the submodel. LOS-only propagation at high gigahertz frequencies means that it is simply impossible to intercept the signal when the eavesdropper is out of range or obstructed in relation to the legitimate transmitter. Thus, in practice eavesdropping even a small number of VSATs in a limited geographical area of tens of square kilometres would require a significant number of colluding eavesdroppers due to these inherent interception range constraints, making the feat rather impractical for even better resourced adversaries.

4.2 Submodel 2a: Beam tracking potential in equatorial orbits

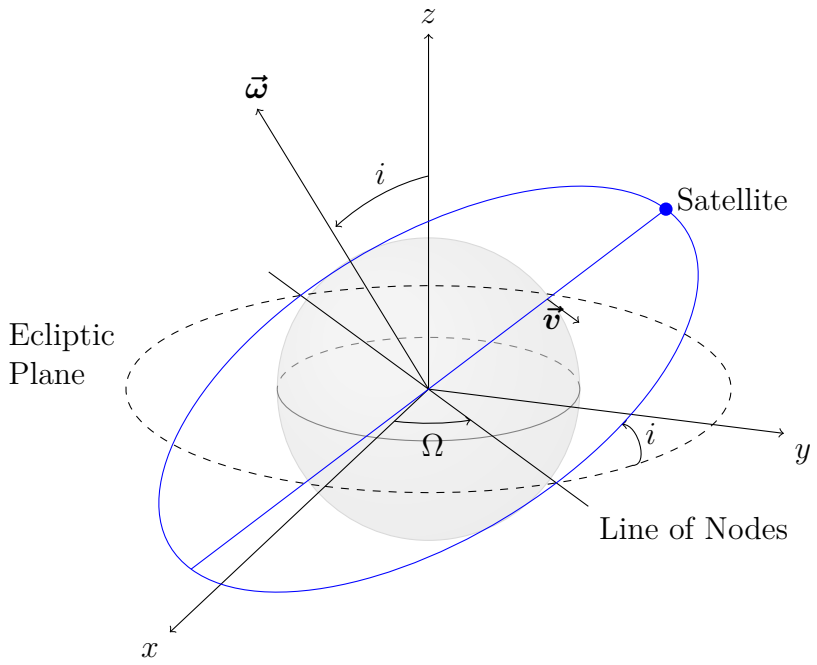

Figure 15: Geometry of a circular Earth orbit.

In addition to being aligned along the LOS of the VSAT's main lobe, the eavesdropper needs to be able to intercept sufficiently long transmission to have a chance to detect a target VSAT transmitter from background noise and potential other active transmitters. 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 a practical example, millisecond-level signal capture may be enough for direction finding applications, while useful insights for proper COMINT would require longer-term interception of a VSAT's UL signal over periods ranging from seconds to days.

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 (vector $\vec{\boldsymbol{v}}$ on figure 15). If this velocity exceeds the cruise speed of the eavesdropper, the airborne platform is not able to continuously follow the UL 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. Figure 15 introduces visually the basic geometry of a circular inclined orbit, as well as some variables relevant to the models 2a and 2b.

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 subtracted from the angular velocity of the satellite, as both share roughly the same rotational axis.

$$T^2 = (\frac{4\pi^2}{GM})r^3 \tag{8}$$

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 measured from the centre of mass of the orbited body.

In essence, the aircraft can be modelled as a low-flying atmospheric satellite. This allows for the same equations to be used in modelling 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

$$\omega_{sat} = \frac{2\pi}{T} \tag{9}$$

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

$$v_r = \omega r \tag{10}$$

As $\omega_{sat} = \omega_{air}$ in the case that the aircraft is able to continuously 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 (8), (9) and (10). Rearranging Kepler's third law to solve for $v_{r,air}$ gives

$$v_{r,air} = r_{air}\sqrt{\frac{GM_E}{r_{sat}^3}} \tag{11}$$

Variables r_{air} and r_{sat} are the orbital radiuses of the eavesdropping aircraft and the receiving satellite measured from the centre of the Earth while M_E is the mass of the Earth. Equation (11) gives $v_{r,air}$ in the Earth-centred inertial (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 Earth-centred – Earth-fixed (ECEF) coordinate system. For circular equatorial orbits, this can be simply achieved by subtracting the spin of the Earth from $v_{r,air}$.

$$v_{r,ECEF} = v_{r,air} - \omega_E r_{air} \tag{12}$$

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

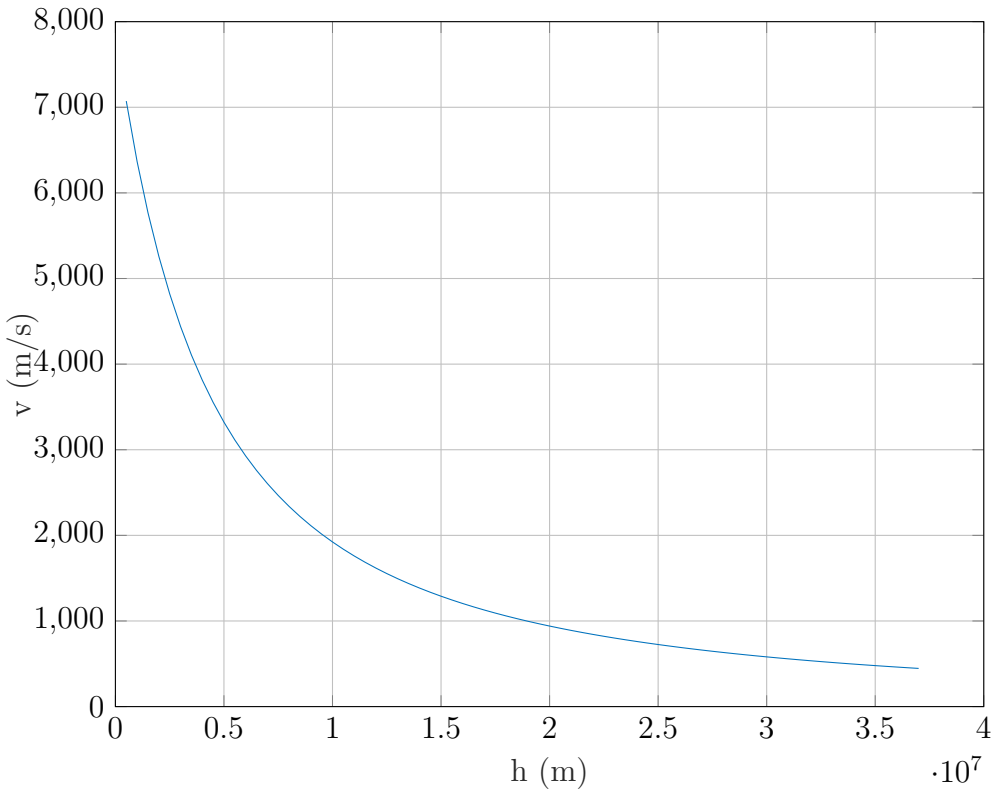

Figure 16: Sub-satellite velocity as a function of orbital altitude (m) in equatiorial orbits.

Figure 16 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 $h_{sat} = [5 \cdot 10^5, 3.7 \cdot 10^7]$. The UT is assumed to have a half-power beamwidth

of 3.5 degrees, the figure for the first-generation blanket-authorised Starlink UT [36]. 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 at 35 786 km. As the graph is computed in the ECEF coordinate frame, sub-satellite velocity approaches zero at GEO altitudes, meaning 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 between 5 and 7 km/s in orbital altitudes between $h_{sat} = [5 \cdot 10^5, 2 \cdot 10^6]$. At these velocities, it is simply impossible for an atmospheric vehicle keep tracking a narrow UL beam of a VSAT. Even fast reconnaissance aircraft, such as the Lockheed SR-71 Blackbird fly at a fraction of these sub-satellite velocities at the maximum velocity of $1\,\mathrm{km\,s^{-1}}$. For reference, high velocity artillery cannons have muzzle velocities in a similar range.

4.3 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 limited when considering relationship of orbital altitude to coverage and latency. This is due to the space segment architecture of modern satellite megaconstellations that aim to achieve worldwide coverage by placing a number of satellites into Earth orbits that are inclined in nature. Often, real-world satellite systems, such as those in appendix A, follow the Walker Star and Delta constellation configurations, whose basic characteristics are outlined briefly in chapter 2.1.2.

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 ECEF coordinate frames. On the other hand, any inclination induces additional velocity component perpendicular to this original equatorial component.

Transitioning from the simple scalar representation into a vector space makes analysing inclined orbital motion less cumbersome. Here, angular velocity is an especially 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 subtracting the rotation vector of the Earth gives angular velocity vector in the ECEF 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

$$\omega_{ECEF} = ||\boldsymbol{R_y}(\theta)\ \vec{\boldsymbol{\omega}}_{\boldsymbol{sat,i}} - \vec{\boldsymbol{\omega}}_{\boldsymbol{E}}||$$

ω_{ECEF} is the scalar angular velocity of the satellite in the ECEF coordinate frame. $\vec{\boldsymbol{\omega}}_{\boldsymbol{sat,i}}$ and $\vec{\boldsymbol{\omega}}_{\boldsymbol{E}}$ are the angular velocity vectors of the inclined satellite orbit and the spin of the Earth. Vector $\vec{\boldsymbol{\omega}}_{\boldsymbol{sat,i}}$ is visaulised in 15 as vector $\vec{\boldsymbol{\omega}}$ perpendicular to the orbital plane of the satellite.

Finally, the sub-satellite velocity figure can be solved based on the scalar angular velocity by applying equation (10), as the altitude of the airborne platform h_{air} and the mean radius of the Earth R_E are known.

$$v_{air} = \omega_{ECEF}\ (h_{air} + R_E) \tag{13}$$

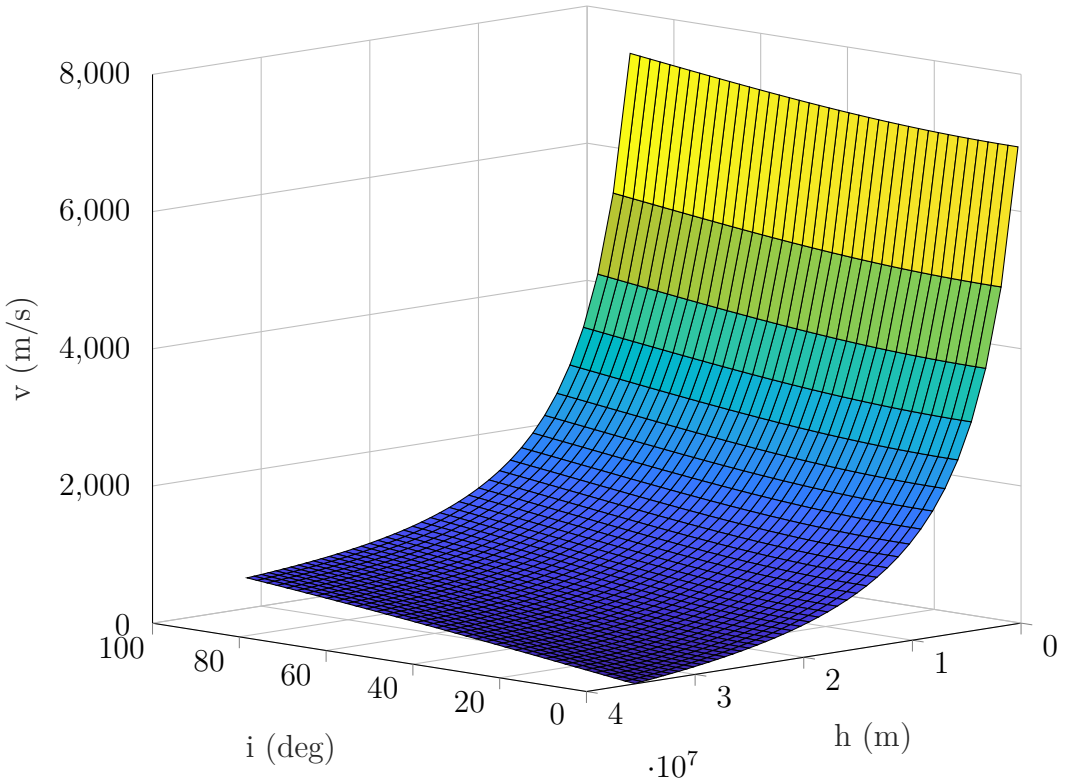

Figure 17: Sub-satellite velocity (m/s) as a function of orbital altitude (m) and inclination (degrees).

Figure 17 shows the sub-satellite velocity of a satellite in an inclined orbit as a function of orbital height and inclination. The resulting sub-satellite velocities in meters-per-second were computed as a function of inclinations in the range $i = [0, 90]$ and orbital heights $h = [500 \cdot 10^3, 37 \cdot 10^6]$. The results show that inclination has a minor influence while the orbital height is the dominant factor determining the sub-satellite velocity. Thus, inclined orbits do not improve the adversary's chances at intercepting and tracking UL transmissions of a VSAT. With velocity ranges in the single digit kilometre-per-second range, even the fastest man-made atmospheric vehicles and projectiles fall short of the sub-satellite velocities of the beam at typical aircraft cruising altitudes.

4.4 Submodel 3: Listening window

Tracking potential is one way to evaluate risk of an airborne adversary trying to intercept and collect useful RF data from UL transmissions of a VSAT. Theoretical length of a capture window, or the listening window of an eavesdropper is a useful metric in evaluating the potential attack types. As mentioned in submodel 2a, different durations of interception have varying implications for the legitimate transmitter. Millisecond-length RF samples may still enable an adversary to geolocate a transmitter while useful insights for proper COMINT would require longer-term interception of a VSAT's UL signal over periods ranging from seconds to days.

Quantitative analysis of the listening window of an eavesdropper is more complex in terms of input parameters that need to be considered. On a high level, the window is primarily influenced by the relative motion between the UL 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 negligible effect when trying to intercept signals to a LEO satellite. 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.

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 ECEF coordinate frame ω_{ECEF}.

$$t_{pass} = \frac{\theta_{beam}}{\omega_{ECEF}} \tag{14}$$

Figure 18 shows numerical results for listening windows computed for a narrower range of orbital periods $T_{orbit} = [5400, 42400]$ seconds. As we can see from 3D plot, the window starts to grow as the period approaches that of a GEO. In theory, the period goes to infinity for satellites in GEO as the sub-satellite velocity matches the rotation of the Earth, making it possible for an aircraft theoretically to indefinitely loiter inside a VSAT beam communicating with the same GEO satellite.

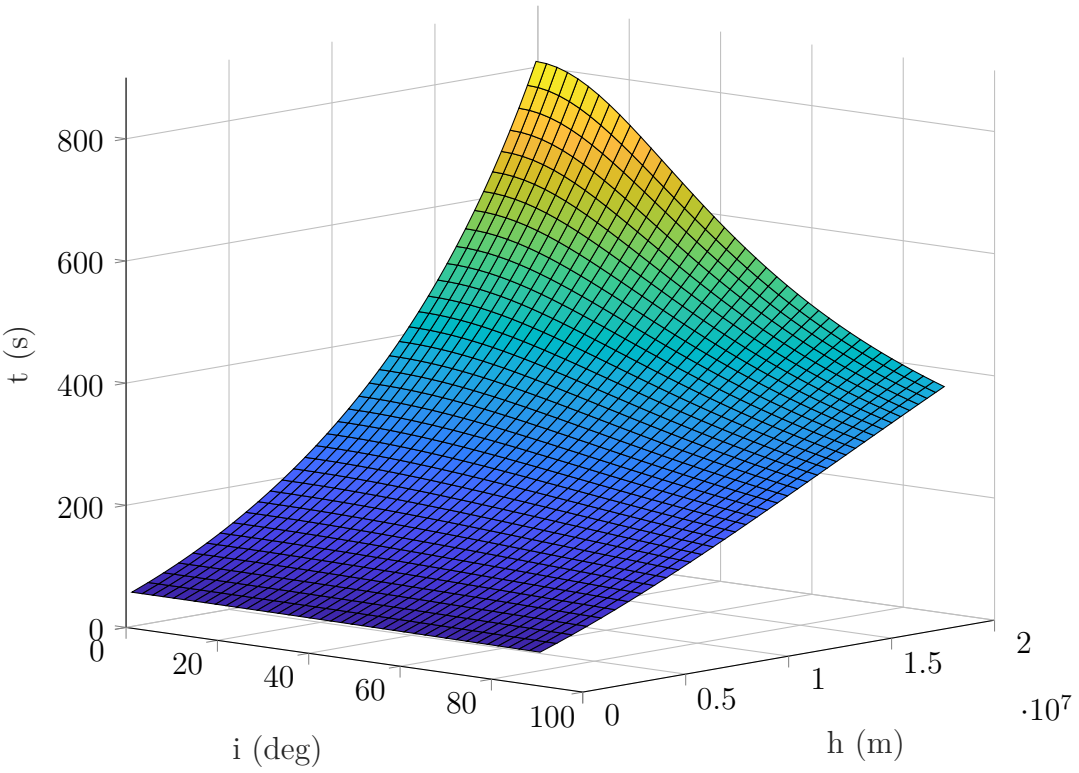

Figure 18: Listening window (s) as a function of orbital altitude (m) and inclination (deg).

4.5 Submodel 4: Jamming link budget

Jamming is the intentional act of drowning out a useful signal relative to the prevailing noise floor with intentional interference. In situations where the jamming dominates over the natural noise sources, the relationship between it and the legitimate signal can be expressed as the signal-to-jamming ratio (SJR). In scenarios with low jamming power, noise sources also need to be considered, resulting in the term signal-to-noise+jamming ratio (SJNR) [52].

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

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

$$S = P_t + G_{tr} - L_t - L_{tr}(R_{tr}) + G_{rt} - L_r \qquad \text{[dBW]} \tag{15}$$

$$J = P_j + G_{jr} - L_j - L_{jr}(R_{jr}) + G_{rj} - L_r \qquad \text{[dBW]} \tag{16}$$

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 [78]. Minimum carrier-to-noise ratio (CNR) requirements for modulation

and coding determine the ability of the jammer to interfere with the legitimate transmission. As discussed in chapter 2.1.3, OneWeb uses adaptive modulation and coding 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 exceptionally low CNR, if significant forward error correction is utilised. [31, 79]

Jamming of the UL 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 simplified scenario allows end-to-end performance of a communications link to be analysed through a link budget, a theoretical calculation where gains and losses of a RF system are summed to compute the figures of merit, such as SNR, spectral efficiency, and theoretical throughput [30]. Table 6 presents an UL link budget for the Kymeta Hawk u8 UT interfacing with the OneWeb LEO megaconstellation. Parameters of the UT are taken from [80] and [81], while parameters for the space segment of the OneWeb constellation are based on the values in [28] and [31] for the first-generation constellation. For the advantage of the legitimate user, the modulation and coding scheme in use is assumed to be the less demanding QPSK with 1/2 forward error correction.

Propagation paths in satellite links inherently cover long distances ranging from hundreds to thousands of kilometres depending on the orbit of the satellite. This type of RF path 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 can be computed in decibels from equation 17 given that an approximate orbital altitude d in meters and UL frequency f in hertz are known.

$$\mathrm{FSPL} = 20\log(d) + 20\log(f) - 20\log(4\pi/c) \qquad [\mathrm{dB}] \tag{17}$$

In addition to FSPL, RF path may experience losses from phenomena like rain, clouds, or atmospheric conditions. It is worth highlighting that the impact of the latter three factors is typically less significant when dealing with Ku and Ka-band propagation over signal paths ranging from hundreds to thousands of kilometres in space. This can be attributed to FSPL increasing with the square of the distance, while the other losses remain constant and significantly smaller in magnitude.

The relative position of the jammer to the receiver's beam pattern is another crucial consideration. In practical scenarios, the jammer may be situated within the receiver's main beam or outside it, resulting in varying gain figures at the receiver's end. More specifically, the jammer can be transmitting within the receiver's main lobe, side lobe, or nulls between them. While the latter can be readily dismissed due to high attenuation, the former two scenarios offer opportunities for the jammer to disrupt the legitimate transmission. The side lobe level of modern constellations remains unknown for both satellites and terminals, but estimations can be derived based on constraints such as the International Telecommunication Union radio regulations, which establish inherent limits for the maximum allowable power flux density. In [82], the authors estimated maximum allowable sidelobe levels for the first-generation Starlink and OneWeb constellations at -32.9 and $-24.0\,\mathrm{dB}$, respectively.

Finally, equation 15 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. Side lobe related losses were ignored in the analysis due to their uncertainty. This allows the propagation losses to be estimated with just the figures of FSPL and atmospheric loss. For the latter, a figure of 0.35 dB from [30] was applied. Signal-to-noise ratio (SNR) was also normalised over 1 Hz of bandwidth.

$$S_{rx} = \text{EIRP} - \text{FSPL} - L_{ath} + \text{G/T}_{sat} \qquad \text{[dBW]} \tag{18}$$

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

Parameter	Value	Notes
Constants		
Atmospheric 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		
FSPL [dB]	176.95	
Channel bandwidth [dBHz]	73.01	
Received power @ sat [dB]	-192.41	
Required jamming power @ sat [dB]	-193.41	$J \gg N$

Jammer's detailed RF characteristics would the next point to consider, and link budget allows these to be examined in the same manner as the legitimate UL of the VSAT. Analysis in table 6 was ended at the receiver of the satellite due to limited information available in the jammer's end. Jamming devices range from handheld

ones all the way from high power vehicle or aircraft mounted systems both stationary and mobile in their mode of operation. It is worth noting that most of the devices are also highly classified military technology, exacerbating the issue of data scarcity.

Despite this, some comments can be made regarding the susceptibility of VSAT systems to UL jamming. Based on the computations, jammer needs to achieve roughly 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 modulation and coding schemes, such as aforementioned 8PSK or 16-QAM, would push the SJR further to the jammer's benefit.

5 Discussion

Critical communication users demand robust solutions, particularly in terms of the CIA triad of confidentiality, integrity, and availability. The historical limitations of satellite communications 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 potential integration of satellite communications into both mission-critical applications, it is crucial to understand the security of these systems from first principles.

In this thesis, quantitative analysis was applied to develop a robust threat model targeting a Walker-type LEO megaconstellation, fixed VSAT ground station, as well as adversarial airborne eavesdroppers and jammers. The research framework comprised four smaller submodels, each of which was explored through a parametric study with a specific dependent variable and a set of independent ones. The foundation of the four submodels 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 satellite systems in relation to various threats.

Going a little deeper into the model structure and results, submodel 1 evaluated the interception range of a VSAT from an aircraft. The submodel investigated the concept of radio horizon, building a trigonometric model by applying the rule of cosines. A model accounting for the curvature of the Earth as well as simplified atmospheric refraction was used to estimate the maximum interception range of the UL transmissions of a VSAT ground station. The findings highlighted the constraints imposed by the Earth's curvature and atmospheric conditions on intercepting satellite signals, making it simply impossible for a high-altitude aircraft to intercept the legitimate signal from distances beyond little over 100 kilometres due to the LOS-only RF propagation of a SHF signal. This means that the threat of an airborne adversary is 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 be able to evade detection and tracking and can thus fly even in a target country's airspace. If these stealthy systems can then collude with each other, these adversarial systems may be able to collect sufficiently long signal samples from even LEO systems with more distributed space segments. On the other hand, effective collusion requires individual adversaries to exchange information that needs to be then post-processed to extract the desired intelligence. Practically speaking, the non-trivial investment into both communications infrastructure and computational processing capabilities is likely to limit the more sophisticated collusion strategies only to the best-resourced adversaries.

Capabilities of the aircraft were further explored in submodels 2a and 2b through the concept of beam tracking potential with the first model focusing on equatorial and the latter on generalised inclined orbits. The submodel outlined the capability of an airborne eavesdropper to track the main lobe of a communication satellite by comparing the cruising velocities of typical man-made platforms to the sub-satellite

velocity of a VSAT beam intersecting the aircraft's flight path at these altitudes. 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 a satellite beam can vary wildly depending on the orbital altitude due to the varying angular velocity. In this sense, numerical results computed for representative platform configurations verified the challenge for atmospheric vehicles to keep pace with the high sub-satellite velocities in LEO, making continuous tracking of an UL beam of a VSAT practically impossible. Findings were similar for both equatorial and inclined orbits with the satellite altitude being the dominating factor in both cases for the sub-satellite velocity.

Submodel 3 shifted focus to evaluating the risk of an airborne adversary intercepting and collecting RF data from UL transmissions of a VSAT by analysing the theoretical length of a capture window crucial for assessing potential attack types ranging from shorter-duration RF geolocation to longer-running COMINT. Like submodels 2a and 2b, submodel 3 was built on the concept of the relative motion between an UL RF beam and the kinematics of an airborne eavesdropper. GEO communications satellites have an inherently fixed beam, which may allow an airborne adversary to intercept a VSAT transmission to one of these satellites over a theoretically indefinite period by just loitering inside the fixed beam. In this sense, the findings highlighted the physical resilience of NGSO systems against this threat vector, especially when considering them in relation to more traditional GEO systems, which allow for easier UL beam tracking and interception.

Legacy GEO systems may allow for a conveniently flying eavesdropper to intercept the UT's data stream endlessly, as the satellites remain in an inherently fixed position in the sky. In [83], 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.

Finally, submodel 4 investigated active measures an adversary might take against a LEO megaconstellation. More specifically, the threat vector of jamming was evaluated by computing a representative link budget for a representative LEO satellite system, in this case the OneWeb generation 1 megaconstellation. Signal-to-jamming ratio (SJR) and signal-to-noise+jamming ratio (SJNR) equations were formulated and a range of factors for link budgeting, such as atmospheric and path losses, as well as modulation schemes used in satellite communication were discussed. The results illustrated the minimum jamming power required for interference, emphasizing the impact of the chosen modulation and coding on the adversary's ability to disrupt legitimate transmissions.

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.

Interestingly, the computed link budget proves that that the jammer and legitimate user tend to be on 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 necessitates the use of more complex modulation and coding 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. Thus, jamming might be the most feasible vector for an adversary to affect LEO satellite communications thanks to geometry of the problem. In some situations, the jammer experiences less path loss thanks to a shorter RF path in comparison to the legitimate transmitter. Still, the enormous 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.

On the other hand, impact of jamming may be reduced by spread spectrum transmission techniques where the source signal is spread over a wider band in the frequency domain. One potential approach is frequency hopping spread spectrum (FHSS) where the carrier frequency is switched rapidly between a set of frequencies based on a code known by both the legitimate transmitter and receiver. FHSS makes transmissions highly resistant to narrowband interference and jamming while also complicating their interception as the adversary may be at an informational disadvantage when it comes to the transmission codes. In practice, effective capture of FHSS signal requires either expensive RF equipment with wideband intercept capabilities or intricate knowledge of the target system and transmission codes utilised by it.

FHSS-like techniques are already employed to some extent in commercial satellite systems, although they tend to not as robust in comparison to existing governmental counterparts. For example, OneWeb system discussed in 2.1.3 employs a beam-hopping strategy with the satellite transmitting at 16 individual beams that the VSAT switches between every 11 seconds. Although this is primarily a measure for improving spectrum efficiency, it brings with it also some FHSS-like physical security qualities.

6 Conclusion and future work

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 wide-scale application of COTS technology, has opened new frontiers of connectivity. In the future, commercial satellite communications are likely to play a crucial role as a complementary solution for terrestrial mission-critical networks, addressing distinct a multitude of use cases varying in their nature, duration, and forecastability.

Critical communications use cases can be divided into permanent, planned temporary and unplanned temporary, with the first primarily catering to regions traditionally challenging to serve, such as sparsely populated rural areas and maritime settings, where terrestrial coverage is limited. Temporary use cases, whether planned or unplanned, cover a diverse range of locations. Planned events, including large gatherings and political summits, demand coverage augmentation and increased capacity. On the other hand, unplanned events, both natural disasters like earthquakes and man-made incidents like airplane crashes, necessitate immediate response, showcasing the versatility of satellite connectivity. The forecastability and duration of these events vary, influencing the choice of technological solutions. Satellite systems, with their global coverage and ability to serve low-density regions, emerge as a cost-efficient complement to traditional terrestrial networks, ensuring connectivity in remote and challenging environments.

However, the rapid roll-out of commercial satellite solutions 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 inherently 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, have demonstrated the feasibility of intercepting satellite traffic.

Security of commercial satellite systems is a young field of study, and much work remains for future researchers. Regarding commercial broadband networks, approaches such as practical waveform studies through open-source black-box reverse engineering could be an interesting approach to study the threat of less resourced adversaries. Here, COTS software-defined radios and satellite TV equipment have already been verified to be somewhat feasible technology platform that even a less-resourced attacker could exploit. Similarly, the physical and network security of the gateways is another interesting topic with less attention in the research literature. Finally, the conceptual-analytical framework applied in this thesis could be further expanded by building a channel-level simulation for the airborne eavesdropping scenario.

To understand the threat posed by airborne adversaries to a VSAT interfacing with a LEO megaconstellation, a research framework consisting of four distinct submodels was developed in this thesis. A quantitative conceptual analytical research approach was followed, employing a first principles approach, each submodel relying

on geometric and kinematic analyses as well as and link budgets was subjected to a parametric study derived for a representative hardware configuration.

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, necessitating large-scale collusion between eavesdroppers for effective COMINT. Additionally, the radio horizon arising from higher minimum elevation angles in VSATs imposes further constraints on eavesdroppers, requiring them to approach close to transmitting terminals for effective UL 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 the legitimate signal is possible to achieve even with simple and inexpensive radio hardware, such as COTS software-defined radios and satellite TV equipment due to the nature of varying path loss based on the jammer's location in relation to the legitimate user. On the other hand, high number of satellites in a LEO system allows for greater redundancy in satellite choice, making it possible to avoid localised jamming by switching to a satellite in a different part of the sky.

All in all, findings of the thesis highlighted the inherent physical resilience of NGSO VSAT systems against both long and short-term signal interception as well as intentional and unintentional jamming. In this sense, the emerging NGSO mega-constellations do not have inherent physical flaws that would directly jeopardise the security of these systems. The results show that the architecture of these systems makes it tough to eavesdrop or disrupt their operation on a system-wide scale, although more localised adversarial actions may still be feasible to some extent. In fact, compared to their predecessors, the distributed infrastructure of the NGSO systems, especially when it comes to the space segment, bring certain advantages that make the systems robust against a multitude of potential threat factors. Satellite networks have exciting potential to enable previously unforeseen commercial connectivity capabilities in traditionally tough-to-serve use cases even in the demanding field of public safety and defence, but robust cybersecurity measures are a key starting point for deployment into these markets. Thus, proper care needs to be taken when implementing solutions involving these technologies, especially when they are placed into systems with previously limited satellite communications integration.

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] EUSPA, "Secure SATCOM Market and User Technology Report," 2023, Issue 1. doi: 0.2878/961897. isbn: 978-92-9206-076-3.

[5] Euroconsult, "Space Economy Report 2022," 2023, 9th edition.

[6] Erillisverkot, "Teknologiatrendit 2022: Mobiiliverkkojen varmentamiseen panostettava, avaruusteknologia kehittyy," May 4 2022. [Online]. Available: https://www.erillisverkot.fi/teknologiatrendit-2022-mobiiliverkkojen-varmentamiseen-panostettava-avaruusteknologia-kehittyy/

[7] 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

[8] 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

[9] 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/

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

[11] 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

[12] 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

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

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

[15] 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.

[16] 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.

[17] 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

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

[19] "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

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

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

[22] 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

[23] 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

[24] Israel Leyva-Mayorga, Beatriz Soret, Bho Matthiesen, Maik Röper, Dirk Wübben, Armin Dekorsy, Petar Popovski, *Non-Geostationary Satellite Communications Systems*. Institution of Engineering and Technology, Dec. 2022. ISBN 9781839535673

[25] J. G. Walker, "Circular orbit patterns providing continuous whole earth coverage," Royal Aircraft Establishment, Ministry of Aviation Supply, Tech. Rep., Nov. 1970.

[26] ——, "Satellite constellations," *Journal of the British Interplanetary Society*, vol. 37, p. 559, 1984.

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

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

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

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

[31] 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

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

[33] 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

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

[35] T. E. Humphreys *et al.*, "Signal structure of the starlink ku-band downlink," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 59, no. 5, pp. 6016–6030, 2023. doi: 10.1109/TAES.2023.3268610

[36] SpaceX Services, Inc., "SpaceX NGSO ESIM aeroconnectivity FCC filing SES-AMD-20210731-01295," Jul. 2021.

[37] Starlink, "Specifications," 2023. [Online]. Available: https://www.starlink.com/specifications

[38] U. C. of Flight Commission, "Military Use of Balloons During the Napoleonic Era." [Online]. Available: https://web.archive.org/web/20121012113457/http://www.centennialofflight.gov/essay/Lighter_than_air/Napoleon's_wars/LTA3.htm

[39] 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

[40] 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

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

[42] 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

[43] 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

[44] 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

[45] 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

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

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

[48] 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

[49] 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

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

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

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

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

[54] "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

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

[56] Erillisverkot, "Trump ja Putin tapasivat turvallisesti," Dec. 3 2018. [Online]. Available: https://www.erillisverkot.fi/trump-ja-putin-tapasivat-turvallisesti/

[57] 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/

[58] 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/

[59] 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

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

[61] Turvallisuuskomitea, "Ennakointi ja varautuminen." [Online]. Available: https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/ennakointi-ja-varautuminen/

[62] F. Snellman, "The European space-based secure connectivity system and issues of control, security and ownership: assessing the compatibility with Finnish legislation and policy," Master's thesis, University of Helsinki, 2022.

[63] M. Stojkovic, "Public safety networks towards mission critical mobile broadband networks," Master's thesis, Norwegian University of Science and Technology, 2016.

[64] H. Kokkoniemi-Tarkkanen *et al.*, "Mission-critical connecitivity over LEO satellites: Performance measurements using OneWeb system," Nov. 2023, manuscript submitted for publication.

[65] A. Dominguez, "Chapitre 5: la résilience du RRF," May 18 2021. [Online]. Available: https://www.linkedin.com/pulse/chapitre-5-la-r%C3%A9silience-du-rrf-alain-dominguez/?originalSubdomain=fr

[66] P. P. Ray, "A perspective on 6G: Requirement, technology, enablers, challenges and future road map," *Journal of Systems Architecture*, vol. 118, p. 102180, 2021. doi: 10.1016/j.sysarc.2021.102180

[67] W. Jiang *et al.*, "The road towards 6g: A comprehensive survey," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 334–366, 2021. doi: 10.1109/OJCOMS.2021.3057679

[68] Jason Rainbow, "AST SpaceMobile's prototype satellite makes first 5G connection," Sep. 19 2023. [Online]. Available: https://spacenews.com/ast-spacemobiles-prototype-satellite-makes-first-5g-connection/

[69] ——, "Lynk Global starts initial direct-to-device services in Solomon Islands ," Nov. 7 2023. [Online]. Available: https://spacenews.com/lynk-global-starts-initial-direct-to-device-services-in-solomon-islands/

[70] 5G Americas, "Update on 5G Non-Terrestrial Networks," Jul. 2023. [Online]. Available: https://www.5gamericas.org/update-on-5g-non-terrestrial-networks/

[71] Puneet Jain, "WG SA2 - Release 18 Update ," Jan. 6 2023. [Online]. Available: https://www.3gpp.org/news-events/3gpp-news/rel18-sa2

[72] 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: 10.1002/ett.4385

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

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

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

[76] 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

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

[78] "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

[79] 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.

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

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

[82] A. Hills *et al.*, "Controlling antenna sidelobe radiation to mitigate ku-band leo-to-geo satellite interference," *IEEE Access*, vol. 11, pp. 71 154–71 163, 2023. doi: 10.1109/ACCESS.2023.3294130

[83] 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 1st generation broadband satellite communications systems

	SpaceX	Eutelsat OneWeb	Amazon	Telesat	SES
Constellation	Starlink	OneWeb	Kuiper	Lightspeed	O3b mPOWER
Number of sats	4408	588	3326	198	11
Status	1st generation deployed, 5627 satellites launched	1st generation fully deployed, 640 satellites launched. Global coverage available January 2024.	No satellites deployed. To be fully deployed by July 2026 per FCC authorisation	Contract for satellite manufacturing announced in August 2023. Deployments planned to start in 2026.	6 satellites operational, 2 planned to be launched in 2024 + 3 more in 2025.
Total throughput [Tbps]	∼88	∼5	∼164	∼10	∼2.7
Per satellite throughput	∼20	∼7.5	∼50	∼50	200–315
User link band	Ku	Ku	Ka	Ka	Ka
Orbit	LEO (550 km)	LEO (1200 km)	LEO (600 km)	LEO (1000–1350 km)	MEO (8062 km)
Satellite mass [kg]	∼260	∼150	∼650	∼700	∼1700
Satellite life [years]	∼5	∼7	5–7	∼10	>10
Latency [ms]	<50	<50	<50	<50	∼150

Source: [4]

B Appendix: Matlab code

```
%% Physical constants

G = 6.673e-11; % universal gravitational constant, m3 * kg-1 * s-2
M_E = 5.9722e24 ; % mass of the Earth, kg
R = 6371008.8; % radius of the Earth, m
Gravitational_parameter_E = 3.986004418e14;
Omega_E = 2*pi / 86400; % earth's rotation in rad / s

% angular velocity vector for Earth's rotation in the ECI coordinate system
Omega_E_vector = [0;0;Omega_E];

%%  Effect of observation altitude to the range of a eavesdropping sensor in
% relation to different elevation angles of the terminal.

d = @(h,ele)(1/2 .* (sqrt(4 .* h .* (h + 2 * R) + 4 .* R.^2 ...
                .* cosd(90+ele).^2) + 2 .* R .* cosd(90+ele)) / 1000);

%% 3D plot of elevation range of 10 deg to 90 deg and observation altitude in
% range of 100 meters to 20 km.

ele = 10:2.5:85; % elevation angle in degrees
h = 0:750:20000; % aircraft altitude in meters

[H, E] = meshgrid(h, ele);

s = surf(E, H, d(H, E));
view(45,30);
ax = ancestor(s, 'axes');
ax.YAxis.Exponent = 0;
ax.ZAxis.Exponent = 0;

xlabel('e (deg)');
ylabel('h (m)');
zlabel('d (km)');

%% Overlaid line graphs in a single plot
ele = 10:2.5:90; % elevation angle in degrees
h = 0:4000:20000; % aircraft altitude in meters

[H, E] = meshgrid(h, ele);

plot(E,d(H,E));
ax2 = gca;
legend('0 km','4 km','8 km','12 km','16 km','20 km');
ax2.XLim = [10,90];
ax2.YLim = [-4,120];
ax2.YAxis.Exponent = 0;
xlabel('e (deg)');
ylabel('d (km)');
grid on;

%% Orbital radius in relation to velocity of the sub-satellite point (in km/s),
% ECI coordinate frame.

v_air = @(h,r_orbit)( (h+R) .* sqrt( (G*M_E) ./ (r_orbit + R).^3 ) );
%%
% Plot the velocity for orbital radius in range of 500 km to 37000 km.

r_orbit = 500e3:500e3:37e6;

[H_air, R_orbit] = meshgrid(h, r_orbit);

p_v_air = plot(r_orbit, v_air(10000,r_orbit));
xlabel('h (m)');
ylabel('v (m/s)');
```

```
grid on;

%% In the case of GEO, Earth's rotation cancels the velocity of the
% sub-satellite point. Next, we will evaluate the effect of orbital period and
% inclination to the velocity of the sub-satellite point. We setup the orbits in
% the ECI coordinate system and account for the Earth's rotation by converting
% to ECF.

inclination = 0:0.04:pi/2; % inclination in rad
orbital_period = 5400:2000:86400; % in seconds

roty = @(t)[cos(t) 0 sin(t); 0 1 0; -sin(t) 0 cos(t)] ;

omega_ECF_magnitude = @(i, T)( norm(roty(i) * ( (2*pi / T) .* [0;0;1] ) ...
                        - Omega_E_vector));

[I_orbit, T_orbit] = meshgrid(inclination, orbital_period);

I_orbit_deg = I_orbit * (180 / pi);

omega_arr = arrayfun(omega_ECF_magnitude, I_orbit, T_orbit);

v_air_arr = R .* omega_arr;

orbital_altitude = (((Gravitational_parameter_E ...
                    * ( T_orbit/(2*pi)).^2).^(1/3)) - R);

s_omega_ECF_norm = surf(I_orbit_deg, orbital_altitude, v_air_arr);

xlabel('i (deg)'); % inclination
ylabel('h (m)'); % orbital altitude
zlabel('v (m/s)'); % sub-satellite velocity
view(-135,10);

%% Listening window at a set beamwidth.

orbital_period = 5400:1000:42400; % in seconds
beamwidth = deg2rad(3.5); % beamwidth in rad

roty = @(t)[cos(t) 0 sin(t); 0 1 0; -sin(t) 0 cos(t)] ;

[I_orbit, T_orbit] = meshgrid(inclination, orbital_period);
I_orbit_deg = I_orbit * (180 / pi); % convert to degrees for plotting

omega_arr = arrayfun(omega_ECF_magnitude, I_orbit, T_orbit);

t_pass = beamwidth ./ omega_arr; % listening window, fixed aircraft

% convert orbital period to altitude for plotting
orbital_altitude = (((Gravitational_parameter_E ...
                    * ( T_orbit/(2*pi)).^2).^(1/3)) - R);

s_omega_ECF_norm = surf(I_orbit_deg, orbital_altitude, t_pass);

xlabel('i (deg)'); % inclination
ylabel('h (m)'); % orbital altitude
zlabel('t (s)'); % maximum listening window / satellite pass
view([-318 10]);

%% Constellation visualisation from TLEs

startTime=datetime("11-Dec-2023 11:00:00"); % oneweb 2023-12-11
endTime=datetime("11-Dec-2023 11:30:00"); % oneweb 2023-12-11

%startTime=datetime("11-Dec-2023 11:00:00"); % starlink 2023-12-11
%endTime=datetime("11-Dec-2023 11:30:00"); % starlink 2023-12-11
sampleTime=60;
```

```
sc = satelliteScenario(startTime, endTime, sampleTime);

constellation = satellite(sc, "oneweb.tle");
%constellation = satellite(sc, "starlink.tle");

set(constellation(1:length(constellation)), ShowLabel=false);
set(constellation(1:length(constellation)), MarkerSize=3);
set(constellation(1:length(constellation)).Orbit, LineWidth=1);
%set(constellation(1:length(constellation)).Orbit, LineColor="none");

viewer3D = satelliteScenarioViewer(sc, Basemap="bluegreen", ShowDetails=true);

%% Adjust camera position
campos(viewer3D, 40, 18);
```