Uplink security against airborne adversaries in non-geostationary satellite communications

Markus Säynevirta

School of Electrical Engineering

Thesis submitted for examination for the degree of Master of Science in Technology.
Espoo 31.7.2023

Supervisor

Asst. Prof. Jaan Praks

Advisor

M. Sc. (Tech) Tapio Savunen

Aalto University
School of Electrical
Engineering

Aalto University
School of Electrical Engineering

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

Author Markus Säynevirta

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

Degree programme Master's Programme in Automation and Electrical Engineering

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

Supervisor Asst. Prof. Jaan Praks

Advisor M. Sc. (Tech) Tapio Savunen

Date 31.7.2023 **Number of pages** 28+2 **Language** English

Abstract

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

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

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

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

Aalto University
School of Electrical Engineering

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

Tekijä Markus Säynevirta

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

Koulutusohjelma Elektroniikka ja sähkötekniikka

Pääaine Elektroniset ja digitaaliset järjestelmät (TARKISTA) **Pääaineen koodi** ELEC3060

Työn valvoja Apul. prof. Jaan Praks

Työn ohjaaja DI Tapio Savunen

Päivämäärä 31.7.2023 **Sivumäärä** 28+2 **Kieli** Englanti

Tiivistelmä

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

Avainsanat Vastus, resistanssi, lämpötila

Preface

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

Espoo, 31.7.2023

Markus Säynevirta

Contents

Symbols and abbreviations

Symbols

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

Abbreviations

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

1 Introduction

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

However, current satellite systems lack widely accepted cybersecurity standards [4]. Wildly varying technical solutions and their proprietary nature has raised a set of potential vulnerabilities. Moreover, the wide-area broadcast nature of satellite transmissions renders them vulnerable to adversarial groups from abroad or even across an entire continent. This was demonstrated in [5] where the feasibility of eavesdropping downlink satellite traffic was proven practically using widely available and relatively inexpensive satellite television equipment. Within the field of wireless communication, one key driver for this development have been. he proliferation of inexpensive signals processing equipment, such as open source and open hardware Software-Defined Radios (SDR). These devices have enabled interaction with satellite systems by not only nation states but also even individual enthusiast-level actors. Moreover, the vulnerabilities in satellite systems are not limited to only the air interface of these commercial systems. Another third-party vulnerability assessment [6] uncovered serious design flaws in the implementation of satellite user terminal firmware, such as backdoors, hardcoded credentials, weak encryption algorithms as well as undocumented and insecure protocols.

Recent adversarial actions against satellite systems and their supporting infrastructure have raised questions concerning the vulnerability of these systems to a range of potential attack vectors, including cyberattacks, as well as the physical destruction of individual satellites or their supporting ground infrastructure. Recent examples include the cyberattack against the KA-SAT satellite network in February 2022 [7] or the cable cut in one of the optical cables connecting the the SvalSat ground station to mainland Norway. 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 [**?**].

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 [4]. The validity of this approach has long been debated within research and industry circles [8], with the recent consensus being that security of a system should never rely exclusively on obscurity [9, 10].

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

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

Although much work has focused on long operational geostationary broadband and non-geostationary narrowband systems, as well as more long term 5^{th} and 6^{th} generation non-terrestrial networks (NTN), little attention has been directed towards the security of emerging LEO broadband systems. Moreover, most of the research on satellite system protection has examined downlink communication between the satellite and different earth stations [11]. Furthermore, more capital-intensive space or airborne platforms have received relatively little attention, with a greater emphasis being placed on the study of ground-based adversaries. Considering this prior history and recent rapid growth, it is important to better understand the security aspects of this rapidly evolving technology.

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

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

2 Background

2.1 LEO megaconstellations

2.1.1 History and recent developments

During the last five years the satellite communications industry has entered into an era of change. The most prominent new trend is the large megaconstellations with hundreds to thousands of satellites in low earth orbit (LEO). These systems have been enabled by the falling costs in space launches and the mass-production of satellite hardware based on COTS technology [12].

While unlikely to widely replace terrestrial solutions, satellite systems have the potential to serve as a complimentary coverage and capacity solution for both commercial and public safety users. These systems could play a part in the ongoing broadband transition of the existing critical communications networks. Public safety users have more stringent requirements for their communication services when compared to the best effort service provided to normal commercial users.

So far the furthest strides in the new telecom constellations have been made by four companies: SpaceX with its Starlink, OneWeb, Telesat and Amazon with its Project Kuiper. SpaceX and Amazon are U.S. companies and Telesat is Canadian, while OneWeb is controlled by its investors from India, the U.K., France and Japan. In addition to them, multiple other actors from around the world have expressed interest in similar projects. These include for example the EU's Secure Connectivity Initiative and the Chinese Guo Wang constellation.

All four projects furthest in development have significant funding behind their concepts and have secured the necessary regulatory approvals for the initial deployments of their systems. As of May 2023, OneWeb has finished its first generation constellation of 648 satellites while SpaceX was still rolling out its much larger first generation constellation of 4408 satellites. Technologically, these constellations are characterised by their employment of dedicated and vendor-specific technologies in their implementation. For example, all four previously mentioned constellations are currently operating or planning to operate on dedicated Ku and Ka-band frequencies. Also, their user equipment is vendor-specific in nature, be they more traditional parabolic or modern flat-panel phased array technology-based very small aperture terminals (VSAT).

Two US companies, Lynk and AST SpaceMobile, are also planning on beaming broadband service from orbit directly to smartphone sized handsets on 5G frequencies. The latter services are less demonstrated and will need significant R&D investment before becoming a viable option, while the prior are already reaching commercial operability in limited geographic regions.

2.1.2 Key technical characteristics

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 three segments. Practically speaking, this requires tackling the overall opti-

misation problem segment-by-segment while taking into account the requirements of the target application. In , the main elements of a LEO satellite system were characterised into distinct space, ground and user segments, which are visualised in figure **??** [13].

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

Ground segment optimisation tends to be more straightforward . Ground station (GS) planning involves placing a number of stations in appropriate locations around the globe. Metrics for evaluation range from the achieved sky coverage and system throughput and link capacity to the overall deployment and maintenance costs of the GS network [13].

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, [13] raises a good example with bandwidth and carrier frequency, where higher numbers are generally desired for example in high-throughput communication applications the opposite are better suited for achieving suitable link budgets for example when navigation satellite systems for challenging urban terrain or indoor use.

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

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

2.1.3 Example system architechtures (OneWeb / Starlink)

The space segment of the OneWeb system comprises a megaconstellation of 648 LEO satellites distributed into 12 polar orbital planes of 49 evenly spaced satellites, as well as a number of in-orbit spares. Operational satellites fly in an inclined polar orbit with an altitude of 1200 km. Each satellite transmits and receives user terminal (UT) traffic via its 16 fixed Ku-band beams, each of which covers a geographic area with dimensions of 1600 km in longitude and 65 km in latitude. Gateway traffic is forwarded to the satellite network portals (SNP) via two identical steerable Ka-band spot beams with a significantly more focused circular coverage pattern [14, 15].

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

the end-to-end configuration of the OneWeb network [15].

Going deeper into the gateway-side architecture, the infrastructure can be further split into three components, which are network data centres (NDC), points-of-presence (PoP) and satellite network portals (SNP). NDCs host the authentication, authorization, policy and UT databases and are deployed in key global locations. PoPs connect the OneWeb network to the Internet and are deployed at key Internet peering points. Finally, SNPs maintain the connectivity to the LEO space segment composed of the OneWeb satellite constellation. They are situated in remote locations around the globe with room for large antenna arrays of 7 to 30 full motion antennas (on average 16) equipped with a 3.5 m Ka-band dish [14].

On the user terminal side, a similar architectural breakdown can be made – the terminal consists of a satellite antenna, receiver and a customer network exchange (CNX) router. The latter connects the terminal to the end-user devices such as laptops or smartphones [14]. RF transmissions received by the satellite antenna are demodulated and converted to a digital data stream by the receiver hardware of the terminal.

As OneWeb is a LEO satellite system, UTs need to track the movements of the orbiting satellites in real-time and handover between them as they move in and out of view in order to maintain constant connectivity. This can be achieved either with traditional steerable dish or more modern phased array antenna designs. With the prior, two apertures may need to be employed for uninterrupted connectivity, as retrace speed of a single aperture is the inherent limiting factor for hand-over time between satellites. On the other hand, phased array antennas require only a single aperture as their electronic switching can be considered almost instantaneous [15].

Continuing with the distinguishing qualities of the OneWeb system, maybe the most significant is the nature of its air interface coverage pattern, also known as the cell layout. In the OneWeb satellite RAN, the cells are inherently varying and mobile, while on the contrary they are practically geographically static and pre-defined in a terrestrial network of fixed eNBs. Consequently, the movement of the UTs (for example equipment mounted on an aircraft or a high-speed train) is relatively slow when compared to the relative velocities of the satellites in orbit. This means that UT handovers happen mostly due to the orbital movement of the satellites rather than the movement of the UT relative to the surface of the earth, which is the dominating cause of UE handovers in terrestrial systems [16].

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 [16]

OneWeb satellite system makes use of a bent pipe architecture for both its forward and return links. In the forward direction, each Ku-band user terminal downlink maps onto a predetermined Ka-band gateway uplink and vice-versa in the return direction [12, 15].

OneWeb satellite system makes use of a bent pipe architecture for both its forward and return links. In the forward direction, each Ku-band user terminal downlink maps onto a predetermined Ka-band gateway uplink and vice-versa in the return direction [12, 15].

2.2 Aerial Platforms

2.2.1 Technical capabilities

2.2.2 Key trade-offs

2.3 Signals intelligence

Signals intelligence (SIGINT) is intelligence gathering through the exploitation of communication systems and noncommunications emitters. Based on the nature of the target system, the discipline of SIGINT can be further subdivided into the sub-disciplines of communications intelligence (COMINT) and electronic intelligence (ELINT) [17] [JP 1-02, JP 2-0 (2013), JP 3-85].

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

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

EOB (WIP / J03-85)

Electromagnetic support (ES) and SIGINT. ES is closely related to, but separate from, SIGINT. The distinction between an asset performing an ES mission or an intelligence mission is determined by who tasks or controls the collection assets, what they are tasked to provide, and for what purpose they are tasked. The distinction between ES and SIGINT is delineated by purpose, scope, and context. Operational commanders task ES assets to search for, intercept, identify, and locate or localize sources of intentional or unintentional radiated EM energy. In contrast, the Director, National Security Agency (NSA)/Chief, Central Security Service, or an operational commander delegated SIGINT operational tasking authority, task SIGINT assets. The purpose of ES is immediate threat recognition, support to planning, and conduct of future operations and other tactical actions such as threat avoidance, targeting, and homing. ES is intended to respond to an immediate operational requirement. ES and SIGINT operations often share the same or similar assets and resources and may be tasked to simultaneously collect information that meets both requirements. That is not to say that data collected for intelligence cannot meet immediate operational requirements. Information collected for ES purposes is normally also processed by the appropriate parts of the intelligence community (IC) for further exploitation after the operational commander's ES requirements are met. As such, it can be said that information collected from the EMS has "two lives." The first is as ES, unprocessed information used by operational forces to develop and maintain SA for an operationally defined period of time. The second is as SIGINT, retained and processed under appropriate intelligence authorities in response to specified intelligence requirements.

2.3.1 Signal detection

2.3.2 Direction finding and radiopositioning

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

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

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

Frequency Difference of Arrival (FDOA): FDOA relies on measuring the frequency differences of signals arriving at different sensors or antennas. FDOA techniques may provide useful information if the signals have specific frequency characteristics or modulation patterns that can be exploited.

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

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

2.3.3 Eavesdropping and traffic analysis

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. [18]

This core principle of secure communications was formalised by Shannon [19] in his 1949 paper through the notion of perfect secrecy achieved through a one-time pad. Shannon's secrecy system assumes that both the intended recipient and the eavesdropper acquire the encoded codeword without any degradation, i.e. the communication channel is error-free. This theoretical assumption applies very rarely to real world systems, where some noise is almost always present. [18]

Wyner [20] expanded on Shannon's original system by exploring the role of noise in the context of secure communications through the channel model called *degraded wiretap channel* (DWTC). The model assumes a situation where the sender (Alice) attempts to communicate with the legitimate recipient (Bob) over a noisy channel.

Simultaneously an eavesdropper (Eve) observes a degraded version of the signal received by the legitimate recipient. [21]

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. [18]

Csiszár and Körner [22] developed a more general approach that they termed the *broadcast model with confidential messages*.

2.4 Critical communications

2.4.1 Technology evolution

2.4.2 Requirements

6.3.1 Network Requirements

Current drives to bring about the benefits of commercial broadband networks to mission-critical service providers have developed solutions “over-the-top” of existing public networks. Doing so is, however, not sustainable in the long-term since the public safety networks desire a level of sophistication that ensures they get priority in the systems (Tata and Kadoch 2014, p. 3). The networks should be managed in the same way that TETRA, TETRAPOL, and P25 works, giving priority bandwidths to public safety networks while ensuring that the communication is encrypted end to end. Even in extreme weather conditions, the dedicated broadband services for the mission-critical services must ensure:

Survival over multiple failures Priority for mission-critical data Offer the desired coverage and capacity Maintain data integrity and ensure end-to-end encryption Be interoperable with other networks to offer solutions when needed Provide the desired support for devices and applications.

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

Confidentiality Integrity Reliability Non-repudiation Authentication.

6.7.8.1 Confidentiality

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

6.7.8.2 Integrity

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

6.7.8.3 Reliability

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

6.7.8.4 Non-repudiation

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

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

2.5 Threat model

2.5.1 Passive and active eavesdropping

Space uplink Ground downlink

The eavesdropper can act both passively and actively. In the prior case

Regarding these two vectors, the research community has been thus far more focused on securing downlink communications from satellites to user terminals and gateways. Here, eavesdroppers have been assumed to be ground based, as space or airborne RF monitoring equipment has been seen as relatively limited in its performance compared to the terrestrial counterparts.

2.5.2 Jamming

2.5.3 Active eavesdropping

2.5.4 Signal geolocation

2.6 Link budgets

2.7 Channel models

2.8 Orbital mechanics

2.8.1 Kepler's laws

Kepler III

$$T^2 = (\frac{4\pi^2}{GM})r^3 \tag{1}$$

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

2.9 Coordinate systems

3 Research material and methods

3.1 Methodology

Conceptual analytical approach.

Research method. Parametric stude of an analytical model.

Järvinen, P. Tutkimustyön metodeista.

3.2 Link budgets

3.2.1 Characteristics of satellite terminals

Beamwidth, gain, EIRP.

3.3 Transmission characteristics of the uplink

Protocols, packet sizes.

4 Threat scenarios in relation to requirements

Tässä osassa kuvataan käytetty tutkimusaineisto ja tutkimuksen metodologiset valinnat, sekä kerrotaan tutkimuksen toteutustapa ja käytetyt menetelmät.

5 Results

5.1 Submodel 1: Interception range

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

Trigonometric tangent function of the interception range triangle is

$$\tan(\theta_{Alice}) = \frac{h_{Eve}}{d_{Eve}} \tag{2}$$

where θ_{Alice} is the minimum elevation angle of the user terminal, h_{Eve} is the operational altitude of the intercepting airborne platform and d_{Eve} is its distance from Alice on the ground, in essence the interception range. Rearranging (2) for d_{Eve} gives

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

Figure 1 shows d_{Eve} in the range $\theta_{Alice} = [10°, 85°], h_{Eve} = [100, 20000]$. In the resulting 3D plot, the x-axis is the minimum elevation angle of the terminal, y represents the altitude of the eavesdropping platform, and z corresponds to the resulting distance between the terminal and the eavesdropping platform. Tangent function has asymptotes at $\theta_{Alice} = \pi/2 + n\pi$ Within the given limits, the asymptotes are not reached and the resulting surface is smooth and continuous. The convex surface exhebits linear growth in relation to altitude h_{Eve} and accelerating tangential growth in relation to θ_{Alice}.

5.2 Submodel 2: Beam tracking potential

On the other hand, the beam movement is primarily driven by the motion of the receiving satellite in orbit, which is in turn governed by Kepler's laws of orbital motion. Tracking capability of the aircraft can be evaluated by analysing the velocity of the sub-satellite point at the eavesdropper's operational altitude (point x on figure 2). If this velocity exceeds the cruise speed of the eavesdropper, the airborne platform is not able to continuously follow the uplink RF beam, which limits the time window into individual satellite passes.

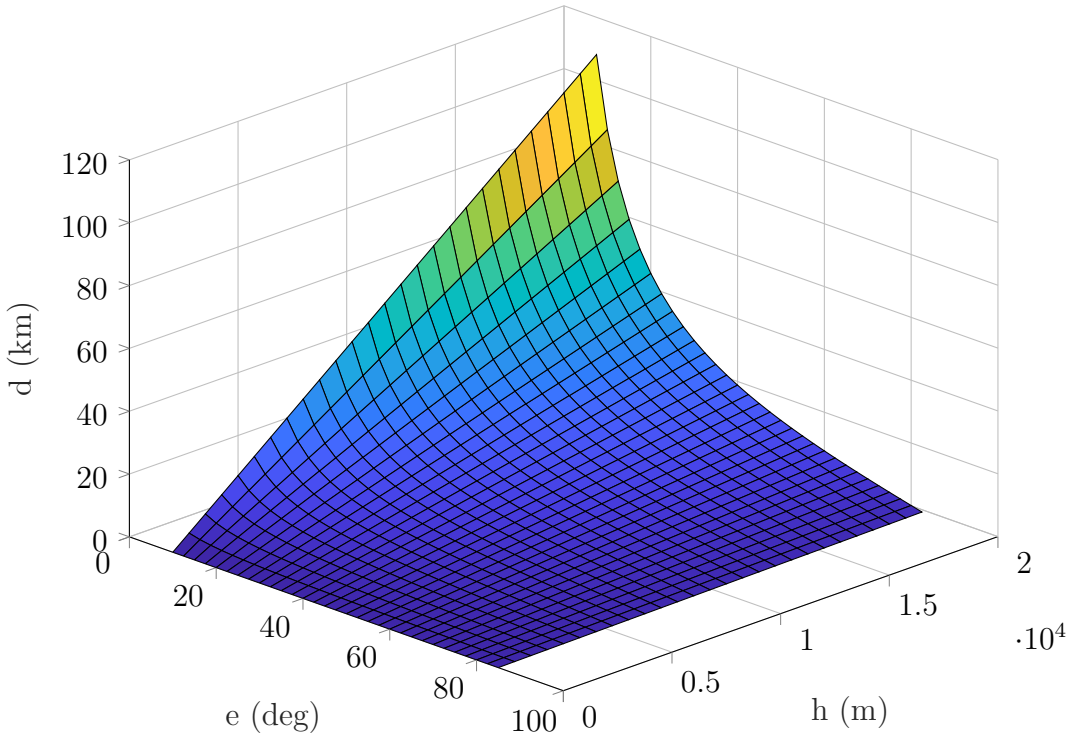

Figure 1: Interception range (d) as a function of minimum elevation angle (e) and operational altitude of the eavesdropper (h).

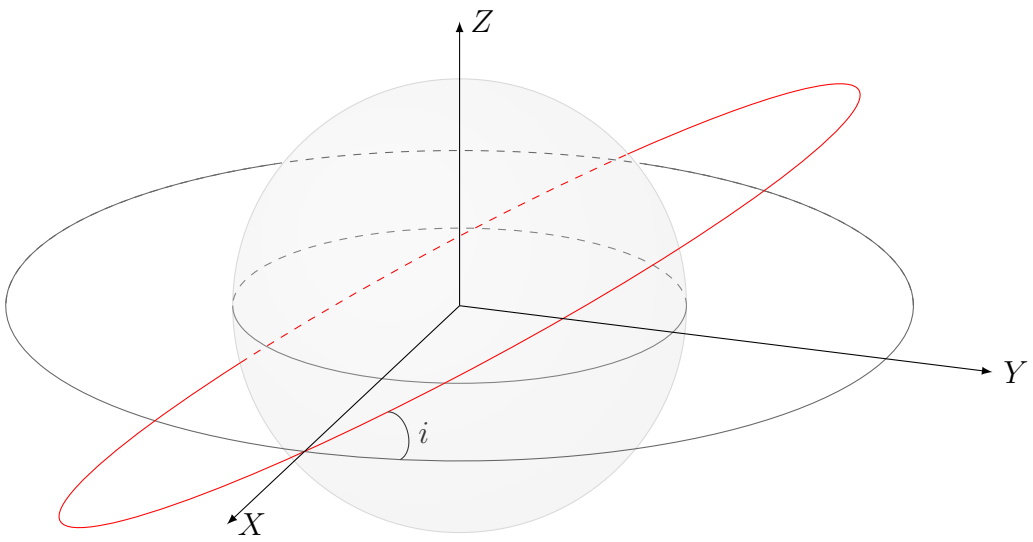

Figure 2: Geometry of a circular Earth orbit.

5.2.1 Equatorial orbits

Communication satellites reside often in circular orbits, which are a special case when evaluating Kepler's laws of orbital motion. Here, the velocity of the sub-satellite point can be computed by solving Kepler's third law for the orbital velocity at a set

altitude. In equatorial orbits, Earth's rotation can be directly substracted from the angular velocity of the satellite, as both share roughly the same rotational axis.

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

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

$$\omega_{sat} = \frac{2\pi}{T} \tag{4}$$

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

$$v_r = \omega r \tag{5}$$

As $\omega_{sat} = \omega_{air}$ in the case that the aircraft is able to continuosly track the satellite, the velocity of the sub-satellite point at the cruising altitude of the aircraft $v_{r,air}$ can be solved by combining equations (1), (4) and (5). Rearranging Kepler's third law to solve for $v_{r,air}$ gives

$$v_{r,air} = r_{air}\sqrt{\frac{GM_E}{r_{sat}^3}} \tag{6}$$

Variables r_{air} and r_{sat} are the orbital radiuses of the eavesdropping aircraft and the receiving satellite measured from the center of the Earth while M_E is the mass of the Earth. Equation (6) gives $v_{r,air}$ in the ECI coordinate frame. To compute the actual movement of the sub-satellite point relative to the surface of the Earth, the velocity figure needs to be converted to the ECF coordinate system. For circular equatorial orbits, this can be simply achieved by substracting the spin of the Earth from $v_{r,air}$.

$$v_{r,ECF} = v_{r,air} - \omega_E r_{air} \tag{7}$$

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

5.2.2 Generalisation to inclined orbits

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

The same analysis methods remain valid for inclined orbits but some additional factors need to be considered. Equatorial orbits have only a single velocity component parallel to the xy-plane in both ECI and ECF coordinate frames. On the other hand,

any inclination induces additional velocity component perpendicular to this original equatorial component. This velocity component is visualised by v_z in figure **??**.

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

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

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

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

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

ω_{ECF} is the scalar angular velocity of the satellite in the ECF coordinate frame. $\vec{\boldsymbol{\omega_{sat,i}}}$ and $\vec{\boldsymbol{\omega_E}}$ are the angular velocity vectors of the inclined satellite orbit and the spin of the Earth. Finally, the sub-satellite velocity figure can be solved based on the scalar angular velocity by applying equation (5), as the altitude of the airborne platform h_{air} and the mean radius of the Earth R_E are known.

$$v_{air} = \omega_{ECF}\ (h_{air} + R_E) \tag{8}$$

5.3 Listening window

Listening window is the time that an airborne eavesdropper is able to intercept the uplink RF transmission from a user terminal on the ground. Analysing this window is somewhat more complex in terms of the model required and potential input parameters that need to be considered. On a high level, the window is primarily influenced by the relative motion between the uplink RF beam of the terminal and the kinematic characteristics of the airborne eavesdropper. The latter include qualities such as cruise speed, operational altitude, manoeuvrability and controllability. They define the ability of the aircraft to keep a lock on the moving RF beam. These are in

turn defined by the characteristics of the platform, a topic discussed in more detail in section 2.2. As demonstrated by the inclination-orbital altitude analysis, aircraft kinematics have very little effect at LEO satellite altitudes ranging from hundreds to couple thousand kilometers. In practice, the great disparity between the velocities makes it possible to abstract away the movement of the aircraft and assume it to be stationary for the sake of analysis.

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

$$t_{pass} = \frac{\theta_{beam}}{\omega_{ECF}} \tag{9}$$

5.4 Listening window

5.4.1 Equatorial orbits

5.4.2 Inclined orbits

5.5 Link budgets

5.5.1 Uplink transmission

5.5.2 Airborne jamming

6 Discussion

6.0.1 Passive eavesdropping

6.0.2 Active eavesdropping

6.0.3 Jamming

6.0.4 Radiolocation

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

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

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

7 Conclusion

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

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

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

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

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

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

Future work? Waveform studies?

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*, 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] 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

[5] 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

[6] 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/

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

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

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

[10] 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.

[11] 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.

[12] 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

[13] 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

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

[15] WorldVu Satellites Limited, "OneWeb LEO K-band NGSO constellation FCC filing SAT-LOI-20160428-00041," Apr. 2016, accessed: 2022-12-22. [Online]. Available: https://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATLOI2016042800041&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

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

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

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

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

[20] 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

[21] 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

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

A Esimerkki liitteestä

Liitteet eivät ole opinnäytteen kannalta välttämättömiä ja opinnäytteen tekijän on kirjoittamaan ryhtyessään hyvä ajatella pärjäävänsä ilman liitteitä. Kokemattomat kirjoittajat, jotka ovat huolissaan tekstiosan pituudesta, paisuttavat turhan helposti liitteitä pitääkseen tekstiosan pituuden annetuissa rajoissa. Tällä tavalla ei synny hyvää opinnäytettä.

Liite on itsenäinen kokonaisuus, vaikka se täydentääkin tekstiosaa. Liite ei siten ole pelkkä listaus, kuva tai taulukko, vaan liitteessä selitetään aina sisällön laatu ja tarkoitus.

Liitteeseen voi laittaa esimerkiksi listauksia. Alla on listausesimerkki tämän liitteen luomisesta.

```
\clearpage
\appendix
\addcontentsline{toc}{section}{Liite A}
\section*{Liite A}
...
\thispagestyle{empty}
...
teksti\"a
...
\clearpage
```

Kaavojen numerointi muodostaa liitteissä oman kokonaisuutensa:

$$d \wedge A = F, \tag{A1}$$

$$d \wedge F = 0. \tag{A2}$$

B Toinen esimerkki liitteestä

Liitteissä voi myös olla kuvia, jotka eivät sovi leipätekstin joukkoon: Liitteiden taulukoiden numerointi on kuvien ja kaavojen kaltainen: Kaavojen numerointi

Table B1: Taulukon kuvateksti.

9.00–9.55	Käytettävyystestauksen tiedotustilaisuus (osanottajat ovat saaneet sähköpostitse valmistautumistehtävät, joten tiedotustilaisuus voidaan pitää lyhyenä).
9.55–10.00	Testausalueelle siirtyminen

muodostaa liitteissä oman kokonaisuutensa:

$$T_{ik} = -pg_{ik} + wu_i u_k + \tau_{ik}, \tag{B1}$$

$$n_i = nu_i + v_i. \tag{B2}$$