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** 19+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** 19+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

Operators

$\nabla \times \mathbf{A}$	curl of vectorin $\mathbf{A}$
$\frac{\mathrm{d}}{\mathrm{d}t}$	derivative with respect to variable t
$\frac{\partial}{\partial t}$	partial derivative with respect to variable t
$\sum_i$	sum over index i
$\mathbf{A} \cdot \mathbf{B}$	dot product of vectors $\mathbf{A}$ and $\mathbf{B}$

Abbreviations

COMINT	communications intelligence
ELINT	electronic intelligence
EO	earth observation
GNSS	global navigation satllite system
ISR	intelligence, surveillance, and reconnaissance
satcom	satellite communication
SIGINT	signals intelligence

1 Introduction

Over the past five decades, satellite systems have undeniably emerged as indispensable enablers of the modern way of life within an increasingly technology-driven human society. Innovation in fields such as global navigation satellite systems (GNSS), earth observation (EO), 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 have 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, the current satellite systems lack widely accepted cybersecurity standards. [1] Wildly varying technical solutions and their proprietary nature has raised a set of potential vulnerabilities. Additionally, the wide-area broadcast nature of satellite transmissions poses its own challenges. Attacks on terrestrial communications infrastructure are typically more localised due to the inherent limitations imposed by the laws of radio propagation. In contrast, satellite systems do not benefit from the same physics-driven protection, rendering them vulnerable to adversial groups from abroad or even across an entire continent.

This was demonstrated in [2] where the feasibility of eavesdropping downlink satellite traffic was proven practically with widely available and relatively inexpensive satellite television equipment. Still, the issues are not only limited to the air interface of these commercial systems. Another third-party vulnerability assessment [3] 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.

These empirical findings arise from the paradigm of "security through obscurity", which the commercial satellite industry has traditionally followed. The model relies on the complexity of the system and limiting of publicly available information on its implementation in securing their systems against potential attacks. However, both researchers and the cybersecurity industry have regarded the paradigm as obsolete for several decades. Within the field of wireless communication, key drivers for this development have been the proliferation of inexpensive signals processing equipment, such as open source and open hardware software-defined radios (SDR), as well as generally more powerful and capable computing hardware.

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

Prior experimental research into the security of traditional satellite broadband

services has revealed serious security vulnerabilities. For example, recent research has proven the

The thesis seeks to answer what kind of risk space-borne uplink eavesdropping poses to modern very small aperture terminal satellite communications. Knowing the history of the field and the prior vulnerabilities with geostationary satcom networks, the current hypothesis is that there could be information leakage happening in the over-the-air communications of the constellation. It is important to understand whether this is happening and if so, to what extent, as it might be possible to extract sensitive user information from these transmissions.

Considering this prior history and the recent rapid growth, it is important to better understand the security aspects of this emerging technology. This thesis will start by delving into the methods of eavesdropping a satellite network. General security architecture of the new LEO broadband services will be discussed in relation to this attack vector. Security of these emerging systems will be explored through a threat model comprising of a Walker-type LEO megaconstellation, fixed very small aperture terminals (VSAT) and airborne eavesdroppers. Overall, the topic will be discussed from the context of the public safety and defence user groups.

The core goal of the thesis is to gain better understanding regarding the security of the over-the-air communications with modern LEO satcom constellations.

The thesis is structured as follows. Section 2 will describe the key characteristics of the examined platforms, in essence LEO megaconstellations and the different aerial platforms. The overall theoretical background is completed by the examination of the discipline of signals intelligence as well as a threat model comprising passive and active eavesdropping, jamming as well as signal geolocation. Section 3 goes over the relevant research material and methods, which is in turn reflected against the previously described threat model in section 4. The results of the simulation are outlined in section 5 and discussed in section 6. Conclusions from the work are described in section 7.

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. [4]

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 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 [1].

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. [5, 6]

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. [6]

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. [5]

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. [5] 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. [6]

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. [7]

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 [7]

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. [4, 6]

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. [4, 6]

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). [JP 1-02, JP 2-0 (2013), NRC-Bulk-Collection]

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

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

2.3.1 Signal detection

2.3.2 Direction finding and radiopositioning

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. [8]

This core principle of secure communications was formalised by Shannon [9] 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. [8]

Wyner [10] 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. [11]

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. [8]

Csiszár and Körner [12] developed a more general approach that they termed the *broadcast model with confidential messages*.

2.4 Threat model

2.4.1 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.

2.4.2 Jamming

2.4.3 Active eavesdropping

2.4.4 Signal geolocation

2.5 Link budgets

2.6 Channel models

3 Research material and methods

3.1 Analysis toolchain

3.1.1 Aerospace Toolbox

3.1.2 Modelling of the HAPS

3.1.3 Modelling of the satellite constellation

3.1.4 Channel model

4 Threat scenarios in relation

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

5 Results

5.0.1 Passive eavesdropping

5.0.2 Active eavesdropping

5.0.3 Jamming

5.0.4 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.

6 Discussion

7 Conclusion

References

[1] 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.

[2] 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

[3] R. Santamarta, "A wake-up call for satcom security," IOActive, Tech. Rep., 2014.

[4] 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

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

[6] 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

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

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

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

[10] 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

[11] 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

[12] 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:

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

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