Universität der Bundeswehr München

Multiuser MIMO Concept for Physical Layer Security in Multibeam Satellite Systems

Matthias German Schraml

Vollständiger Abdruck der von der Fakultät für Elektrotechnik und Informationstechnik der Universität der Bundeswehr München zur Erlangung des akademischen Grades eines

Doktor-Ingenieurs (Dr.-Ing.)

genehmigten Dissertation.

Vorsitzender:	Univ.-Prof. Dr.-Ing. habil. Thomas Weyh
1. Gutachter:	Univ.-Prof. Dr.-Ing. Andreas Knopp, MBA
2. Gutachter:	Univ.-Prof. Dr.-Ing. Armin Dekorsy, Universität Bremen

Die Dissertation wurde am 16.02.2023 bei der Universität der Bundeswehr München eingereicht und durch die Fakultät für Elektrotechnik und Informationstechnik am 11.07.2023 angenommen. Die mündliche Prüfung fand am 26.07.2023 statt.

Abstract

In satellite communications (SATCOM) downlinks, physical layer security (PLS) is challenging to achieve due to their broadcasting nature and line-of-sight channel characteristics. This work investigates the potentials and benefits of a multiple-reflector (MR) antenna scheme in geostationary satellite systems for key-less PLS. Multiple antennas on a satellite essentially unlock the space domain as a further physical resource besides time, frequency and polarization. The exploitation of the spatial degree of freedom enables multiuser multiple-input multiple-output (MU-MIMO) as a convenient signaling strategy for SATCOM providers. In an MU-MIMO system, the receivers do not need to be synchronized and the interference is utilized for eavesdropping protection.

In this work, an overview and fundamentals on PLS and the most common secrecy metrics is provided and their suitability for geostationary SATCOM is discussed. Two precoding algorithms to secure the downlinks of multiple users against multiple eavesdroppers are developed. Their optimization objective and constraints are chosen to perfectly fit the scenario of a geostationary satellite providing secure fixed satellite service. Zero-forcing precoding will be used as a performance reference and demonstrates how much capacity must be sacrificed for security. The goal of the precoding algorithms for security is to generate a channel condition such that the legitimate users receives the signal in higher quality than all eavesdroppers and, thus, fulfilling the requirement of key-less PLS. The utilization of artificial noise is included for improved security performance. Since both precoding algorithms are complicated to solve in the direct form, a reformulation to a convex form is provided to be solvable in polynomial time with off-the-shelf numerical programs. Numerical simulations demonstrate the effectiveness of the precodings and that a MR antenna design provides a significantly higher secrecy performance when compared to a single-reflector design due to the additional degrees of freedom, exhibited by the signal phases.

Kurzfassung

Im Downlink von Satellitenkommunikation ist physikalische Übertragungssicherheit (PLS) aufgrund großflächiger Ausstrahlung und direkter Sichtverbindung nur schwierig zu gewährleisten. In dieser Arbeit werden die Möglichkeiten und Vorteile von mehreren Reflektorantennen an einem geostationären Satelliten für die verschlüsselungsfreie PLS untersucht. Im Wesentlichen eröffnen mehrere Satellitenantennen den Raum neben Zeit, Frequenz und Polarisation als weitere physikalische Dimension. Die Ausnutzung der dadurch zusätzlich gegebenen Freiheitsgrade ermöglicht den Anbietern von Satellitenkommunikationsdiensten die komfortable Übertragungsart Multiple-Input Multiple-Output für mehrere Nutzer (MU-MIMO). In einem solchen MU-MIMO System müssen die Empfänger nicht synchronisiert werden und die auftretende Interferenz wird zum Schutz vor Abhörern verwendet.

Diese Arbeit stellt eine Übersicht und Grundlagen von PLS sowie gängige Metriken der Informationssicherheit bereit und erörtert deren Eignung für die geostationäre Satellitenkommunikation. Es werden zwei Algorithmen zur Signalformung entwickelt, um die Inhaltsdaten von mehreren Nutzern gegen mehrere Abhörer abzusichern. Die Zielsetzung und Randbedingungen der Optimierungsalgorithmen wurden passgenau zum Szenario eines geostationären Satelliten mit sicherem ortsfesten Satellitenfunkdienst ausgewählt. Als Referenz wird Zero-Forcing Signalformung herangezogen, die aufzeigt, auf wie viel Leistung verzichet werden muss, um Sicherheit zu erreichen. Das Ziel der Signalformungsalgorithmen zur Gewährleistung von Sicherheit ist es, Übertragungskanäle zu schaffen, sodass der rechtmäßige Nutzer sein Signal in einer besseren Qualität empfängt als alle Abhörer und somit die Bedingung für verschlüsselungsfreie PLS erfüllt wird. Hinzufügen von künstlich erzeugtem Rauschen steigert die Leistungsfähigkeit in Bezug auf Sicherheit. Da beide Algorithmen in der direkten Formulierung aufwändig zu berechnen sind, wurden sie in eine konvexe Form gebracht, dessen Lösung mit gängigen numerischen Programmen mit polynomiellem Zeitaufwand berechnet werden kann. Numerische Simulationen zeigen die Wirksamkeit der Signalformungsalgorithmen und dass mehrere Satellitenantennen einen deutlich Leistungsgewinn bei der Sicherheit gegenüber Einzelantennen erreichen. Ermöglicht wird das durch die zusätzlichen Freiheitsgrade in der Signalphase.

Danksagung

An dieser Stelle möchte ich mich bei allen bedanken, die diese Arbeit ermöglicht haben.

Mein besonderer Dank gilt Professor Andreas Knopp für die Betreuung dieser Dissertation. Du hast mir die Chance gegeben, trotz meiner Vollzeitbeschäftigung in einer Behörde, als Doktorand zu arbeiten. Ich danke dir für dieses Vertrauen und für die Freiheit, ein Thema zu finden, das diesem Umstand gerecht wird. Dein fachlicher Rat half mir immer, den richtigen Kontext für Veröffentlichungen zu finden. In den vergangenen knapp 10 Jahren habe ich so viel von dir gelernt.

Meinem Zweitprüfer Professor Armin Dekorsy danke ich für die Möglichkeit, meine Arbeit in seinem Institut in Bremen vorzustellen. Die anschließende Diskussion empfand ich als hilfreich, um auch zukünftig in einer potentiellen wissenschaftlichen Karriere die richtigen Fragen stellen und den eigenen Ansatz weiter verallgemeinern zu können.

Allen Mitarbeiterinnen und Mitarbeitern am Institut für Informationstechnik danke ich für den Einblick in spannende Forschungsfragen, den fachlichen Austausch und die schöne gemeinsame Zeit. Besonders erwähnen möchte ich hier die großartige Unterstützung bei administrativen Angelegenheiten, die für mich als externen Doktoranden oft nur durch eure Unterstützung zu bewältigen waren.

Desweiteren möchte ich meinem Sachgebietsleiter dafür danken, mir die Betreuung von Abschlussarbeiten während der Dienstzeit zu ermöglichen. Die Professoren Thomas Latzel und Klaus-Peter Graf haben diese Abschlussarbeiten nicht nur bewertet, sondern auch mit begleitet und mich so an ihrer langjährigen Erfahrung teilhaben lassen.

Von ganzem Herzen bedanke ich mich bei meinen Eltern für eure Unterstützung und euren Rückhalt, der es mir ermöglichte, diese Doktorarbeit nebenberuflich zu schreiben. Meinem Bruder und meinen Freunden danke ich für die Männerrunden und gesellige Abende an den Wochenenden, um den Kopf auch mal frei zu bekommen.

Nicht zuletzt bedanke ich mich bei meiner Freundin Vanessa. Du hast mich in der anstrengenden Endphase aufgemuntert, warst verständnisvoll und geduldig, aber auch bemüht, für einen Ausgleich zu den langen Abenden vor dem Rechner zu sorgen.

Dankeschön

Contents

1 Introduction

1.1 Fixed Satellite Service

Satellites in the Geostationary Earth orbit (GEO), which is about 36 000 km above the Earth's equator, can cover about 40 % of the Earth's surface [MBS20]. Three GEO satellites are sufficient to cover the whole world except the polar regions. Therefore, they can bridge large ranges at reasonable costs without a need of terrestrial radio or cable based infrastructure which is a big advantage of geostationary satellite communications (SATCOM). Millions of households have mounted a small dish antenna on the roof pointing towards the sky to receive broadband fixed satellite services (FSSs), e.g. television broadcasting. Even though the traffic moves from broadcasting to unicast Internet access (or any Internet Protocol based services), the advantages of GEO SATCOM persist. Potential use cases for unicast SATCOM are traffic offloading to the network edges, backhauling or direct broadband access to remote areas. Moreover, GEO high throughput satellites (HTSs) can be combined with low Earth orbit (LEO) constellations in hybrid architectures to offer wide coverage of 5G and Beyond-5G communications [LSR+20]. HTSs with a throughput of hundreds of Gb/s are already state of the art, e.g. *Viasat-2*. Therefore, the design of contemporary HTSs consists of a high number of beams (cells) employing a four-color frequency reuse (FR4) pattern where neighboring beams transmit on different frequency or polarization [FTA+16]. A beam diameter is typically in the range of hundreds of kilometers up to the whole hemisphere mainly depending on the carrier frequency. Fig. 1.1a exemplarily shows the FR4 pattern where four beams are illuminated by a combination of the two carrier frequencies as well as right-hand circular polarization (RHCP) and left-hand circular polarization (LHCP). Hence, the communication via satellites provides ubiquitous services to millions of users that might be hundreds of kilometers apart. On the other hand, the signals are prone to be overheard by unauthorized users. The broadcast property of the wireless channel is contradicting the goal of secret transmission of messages to a legitimate receiver. An eavesdropper within each beam can potentially overhear all messages transmitted to users in the respective beam.

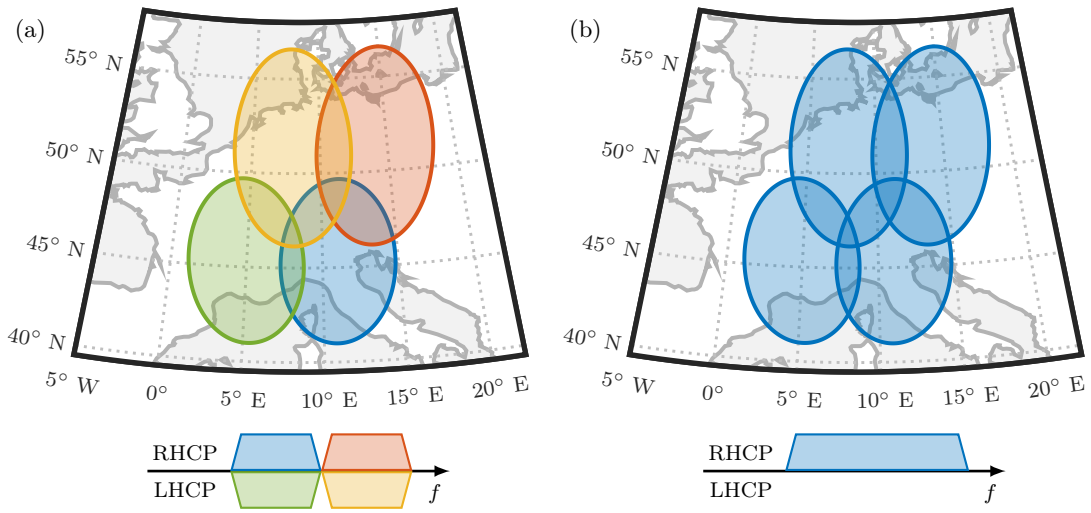

Figure 1.1: Satellite beams on Earth with (a) four-color frequency reuse scheme and (b) full frequency reuse scheme

1.2 Wireless Communications Security

Without protective measures, it is impossible to guarantee the confidentiality of information in wireless channels in general. The common approach is to apply encryption algorithms on higher layers to prevent the interception of user data on the way to their destination. Cryptographic methods are based on mathematical operations like factorization of prime factors [RSA78]. They are said to be computationally secure because the effort for an attacker to decrypt the information exceeds the computational performance of present systems. However, with the advent of new computing power, especially future quantum computers, such algorithms will not be secure anymore [Sho97].

In contrast to key-based cryptographic security, physical layer security (PLS) can achieve information-theoretic security which is now commonly accepted as the strictest form of security [BD06]. The concept of key-less PLS is based on the fact that the adversary receives the message over a degraded version of the channel outputs compared to the legitimate user [Wyn75]. Moreover, cryptography and PLS can work hand in hand to increase the difficulty of the attack on cryptographic systems or make it altogether impossible [HM09].

The early theoretical frameworks on PLS [Wyn75; LH78] were not directly applicable to practical systems. With the development of enabling techniques like, for example, channel coding, channel-based adaption and injection of artificial signals, the research on PLS in terrestrial wireless systems intensified [HFA19]. PLS is a promising technology for the security needs of Beyond-5G networks [WKX+18] which includes mmWave and

multiple-input multiple-output (MIMO) communications with a huge number of antennas, i.e. massive MIMO. The survey [WBZH19] provides a comprehensive overview on the optimization and design of PLS systems. However, most publications for terrestrial PLS exploit the randomness of the wireless channel response between a base station and its users or eavesdroppers.

The SATCOM channel is not comparable to a terrestrial link especially due to its dimension and the use of directional antennas. The propagation conditions for the electromagnetic waves differ substantially. In general, PLS in SATCOM is difficult, since neither multipath components nor interference exist in almost all scenarios, and the line-of-sight (LOS) signal component is the dominant propagation mechanism.

1.3 Security in FSS Satellite Communications

In this thesis, PLS in FSSs with GEO satellites is addressed. The key literature on the state of the art in this particular application is, therefore, summarized in Table 1.1. The multibeam approaches assume a full frequency reuse (FFR) pattern where all beams share the same (full) frequency band and a common polarization. An exemplary FFR beam scheme is shown in Fig.1.1b with right-hand circularly polarized signals on a single carrier frequency. The resulting interference is one of the prerequisites to achieve PLS. Different secrecy metrics are applied to measure the PLS performance, e.g. the secrecy capacity which is the difference of the user capacity and the eavesdropper capacity. The secrecy metrics are explained in detail in Section 2.2.

The only paper utilizing spatial modulation to increase the bit-error rate (BER) at the eavesdroppers is [WSKK18]. In spatial modulation, the data symbols are transmitted in different beams whereas the beam index contains some of the information. In contrast to the user, the eavesdropper is unable to decide in which beam the data symbol has been transmitted and, thus, cannot recover the full information. All remaining works perform precoding to obtain secrecy. Precoding is the process of modifying the phase and amplitude of a data signal for each antenna element of an array in order to generate constructive and destructive interference in the wavefront. In general, a data signal is mapped onto an antenna array such that the multiple radiated signal interfere with each other in a beneficial way. A basic example of precoding is conducted in the next section. In [ALYZ18], the secrecy outage probability and average secrecy capacity are analyzed in a single beam scenario with a single user and a single eavesdropper, each equipped with multiple receive antennas. Furthermore, the sum secrecy capacity under a total transmit power constraint is optimized in [LAL19] where each user is wiretapped by a

Table 1.1: Comparison between existing PLS works for Fixed Satellite Service Downlinks

Work	Beam Scheme	ME	Channel Model	Degree of Freedom	Security Metric
[WSKK18]	Multibeam Single User	✓	LOS	Amplitude	Bit Error Rate
[ALYZ18]	Single beam	–	Shadowed Rician	Amplitude	Secrecy Outage Prob. Average Secrecy Capacity
[LAL19]	Multibeam Multiuser	part	LOS with rain fading	Amplitude	Sum Secrecy Capacity
[LLO+19]	Multibeam Multiuser	–	LOS with rain fading	Amplitude	Min. Secrecy Capacity
[LYO+19]	Multibeam Single user	✓	LOS with rain fading	Amplitude	Secrecy Energy Efficiency with SNR requirement
[GAZ+20]	Single beam	–	Shadowed Rician	Amplitude	Secrecy Outage Prob. Average Secrecy Capacity
[LHVH11]	Multibeam Multiuser	–	LOS	Amplitude	Secrecy Rate Constraint
[ZAO12]	Multibeam Multiuser	✓	LOS	Amplitude, Artificial noise	Secrecy Rate Constraint
This Thesis	Multibeam Multiuser	✓	LOS MIMO	Ampl., Phase, Artificial noise	Min. Secrecy Capacity Security Gap

corresponding eavesdropper. In [LLO+19], the maximization of the minimum secrecy capacity between multiple users and a single eavesdropper under the total transmit power constraint is studied. The authors of [LYO+19] maximize the secrecy energy efficiency to serve a single earth station with a predefined signal-to-noise ratio (SNR) under secrecy constraints set for the eavesdroppers. A threshold-based scheduling scheme to provide PLS in single beam SATCOM is proposed in [GAZ+20]. A joint power control and precoding algorithm, i.e. zero-forcing (ZF) precoding with eavesdropper nulling, in a multiuser scenario with a single eavesdropper is studied in [LHVH11]. In [ZAO12], an algorithm to minimize the total transmit power while maintaining an individual secrecy constraint for each user surrounded by multiple eavesdroppers is developed. Moreover, artificial noise (AN) is considered as an additional technique to increase PLS, as in some cases precoding alone has shown to be insufficient to achieve perfect secrecy. The idea is to enhance the secrecy capacity by limiting the effect of the added AN on the intended user's SNR while significantly degrading that of the eavesdropper.

The identified security gains of the previous works are derived with a LOS channel described by the plane wave model shown in Fig. 1.2a. The plane wave model is common

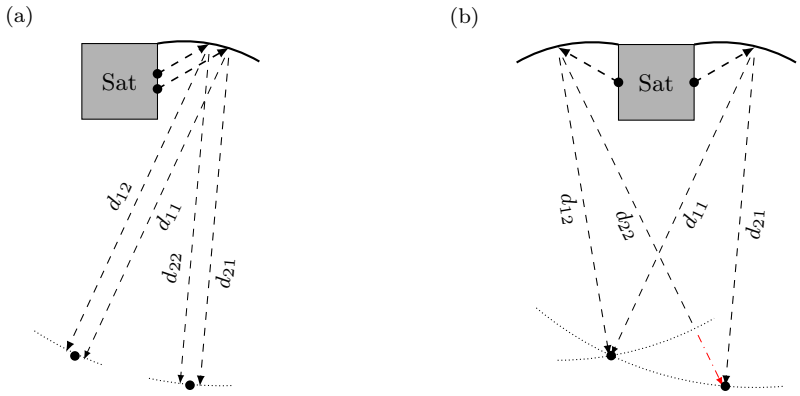

Figure 1.2: Modeling the satellite LOS channel: (a) the plane wave model for a SR satellite and (b) the spherical wave model for a satellite with MR antenna design

for multi-antenna communications when the receivers are far away from the transmitter with narrow antenna spacings. It is assumed that there is no relevant phase difference between the impinging waves of two beams at a receiver, i.e. $d_{11} \simeq d_{12}$ for example in Fig. 1.2a. The plane wave model is sufficient for satellites comprising single-reflector (SR) antenna designs. However, only different amplitudes and powers are available as degree of freedom for precoding. The use of the spherical wave modeling approach illustrated in Fig. 1.2b is necessary to correctly capture all relevant physical effects for MIMO in LOS channels [BOO09], especially for multiple-reflector (MR) antenna designs on the satellite. Dependent on the receiver position on Earth, the signal phase per beam differs due to variable radio path lengths, e.g. $d_{21} \neq d_{22}$ in Fig. 1.2b. This offers another degree of freedom for precoding. A short introduction to LOS MIMO in SATCOM is provided in the next section.

1.4 MIMO Satellite Communications

The contemporary HTS *Viasat KA-SAT*, for example, employs multiple antennas on the satellite [FTA+16]. Moreover, as spectrum is a scarce resource, future generations may adopt the FFR scheme to achieve even higher throughputs [PVS+19]. Essentially, a satellite provider is allowed to transmit in a certain frequency band and compared to the FR4 pattern where two signals per polarization share the bandwidth, only a single signal utilizing the full bandwidth is transmitted in the FFR scheme. Multiple antennas on a satellite and the application of the FFR scheme unlock the space domain as a further physical resource besides time, frequency and polarization. The space domain is accessible because of the position-dependent signal phases as illustrated with the spherical

wave model in Fig. 1.2b. When certain antenna arrangements are fulfilled, the signal phases at the receivers form orthogonal channels and LOS MIMO SATCOM becomes possible [Sch19]. With satellite reflectors separated only a few meters on the spacecraft in an orbit at about 36 000 km altitude, the receivers must be located tens or even hundreds of kilometers apart on Earth to obtain unique channel vectors [Sch19]. Synchronizing two receiver over such a large distance to perform MIMO signal processing is a huge challenge. Multiuser MIMO (MU-MIMO) combines MIMO transmission with signal precoding strategies in order to shift the joint processing to one link end (typically the transmitter) and, thus, avoid the synchronization burden on the other link end [SDSK19]. The gains provided by the spatial domain can now be accessed while the receiver terminals (users) can stay unsynchronized. However, the receivers must provide feedback of their channel state information to the transmitter. The testbed and field trial of a MU-MIMO SATCOM downlink scenario in [SSK20] demonstrate the successful transmission of two independent video signals.

Example: 2×2 MIMO Processing

An ideal LOS MIMO channel applying the spherical wave model shown in Fig. 1.2b is assumed for a basic (multiuser) MIMO processing example. The radio path lengths d_{11}, d_{12}, and d_{21} from the reflectors to the receiver nodes are each an integer multiple of the carrier wavelength λ_c, i.e. $d_{11} = d_{12} = d_{21} = n\lambda_c,\ n \in \mathbb{N}_0$ for example. However, path d_{22} is slightly longer such that $d_{22} = d_{21} + (i + 0.5)\lambda_c,\ i \in \mathbb{N}_0$. For convenience, the attenuations of all channels are equal. Deterministically calculating the phases of the pure LOS paths with lengths d_{11} to d_{22} leads to a vector of channel propagation coefficients, i.e. the channel state information (CSI), of [1 1] for node 1 and [1 −1] for node 2 due to fact that there is a half wavelength difference[1] in the LOS path d_{22}. Details on the LOS SATCOM channel for FSSs are provided in Section 3.2. The nomenclature for the example is the following: s_k is a signal containing data, x_k is the uplink to the satellite and the signal radiated by the kth satellite antenna, and y_k is the signal received at the kth node on Earth. Two kinds of MIMO spatial multiplexing techniques to transmit independent data signals at the same time in the same frequency band and the necessary processing are compared:

Receive Equalization The gateway uplinks the two data signals directly to the satellite, i.e. $x_1 = s_1$ and $x_2 = s_2$. Due to the assumed LOS MIMO downlink channel, the

[1] A radio path of a half wavelength induces a phase shift of π and $e^{j\pi} = -1$.

two nodes on Earth receive the signals

$$y_1 = \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = x_1 + x_2 = s_1 + s_2,$$
$$y_2 = \begin{bmatrix} 1 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = x_1 - x_2 = s_1 - s_2$$

which are a mixture of both data signals. To recover the data signals s_1 and s_2, the two nodes must share the received signals and perform the equalization

$$0.5y_1 + 0.5y_2 = 0.5(s_1 + s_2) + 0.5(s_1 - s_2) = s_1,$$
$$0.5y_1 - 0.5y_2 = 0.5(s_1 + s_2) - 0.5(s_1 - s_2) = s_2.$$

The advantage is that the gateway does not need to know the current channel conditions, but the main drawback are receivers which must be synchronized over hundreds of kilometers.

Transmit Precoding The gateway knows the CSI by feedback of the nodes and can modify (precode) its uplink signals accordingly, i.e. uplinks the two signals

$$x_1 = 0.5s_1 + 0.5s_2,$$
$$x_2 = 0.5s_1 - 0.5s_2$$

to the satellite. The two nodes receive now

$$y_1 = \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = (0.5s_1 + 0.5s_2) + (0.5s_1 - 0.5s_2) = s_1,$$
$$y_2 = \begin{bmatrix} 1 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = (0.5s_1 + 0.5s_2) - (0.5s_1 - 0.5s_2) = s_2$$

which are already the desired data signals. The advantage of precoding are independent (and unsynchronized) receivers with the small drawback of required CSI feedback.

This basic example demonstrates the possibilities of a MR satellite system with MIMO processing. Additionally, a system with transmit precoding can be a MU-MIMO system as a consequence of the fact that the two nodes can be independent users. The receive equalization and transmit precoding are the inverse of the channel in this basic example. Common processing methods to remove the distortions due to the MIMO channel are

presented in [JUN05]. In general, the optimal precoding strategy is strongly dependent on the objective and constraints of the system. In this thesis, the goal is the physical layer security in a MU-MIMO SATCOM system in the geostationary orbit.

1.5 Contributions of this Thesis to Satellite Communications Security

1.5.1 Summary

Modern system concepts such as HTSs with MR multibeam antennas and the use of FFR between the beams offer new possibilities for SNR-based PLS in SATCOM which are not achievable with conventional satellite systems. The exploitation of the spatial degree of freedom for eavesdropping protection in MIMO SATCOM links has first been proposed in [KSL13]. However, the necessity to synchronize the two receiving earth stations is a high burden for practical implementations as proposed in this early concept. A more convenient signaling strategy for SATCOM providers is nowadays the MU-MIMO concept. The MU-MIMO approach based on the fundamentals of MR SATCOM to improve PLS proposed in this thesis elegantly overcomes the drawbacks of missing channel randomness and complicated receiver synchronization and provides significant secrecy gains. A very recent survey paper on PLS in SATCOM [AAE23] acknowledges the uniqueness of the attempt to leverage the MU-MIMO SATCOM for PLS conducted in [SSK21] which is an excerpt of the results of this thesis.

The rest of the thesis starts with an overview and fundamentals on PLS and the most common secrecy metrics in Chapter 2. The suitability of the secrecy metrics for FSS SATCOM is discussed and two fitting metrics are chosen for optimization and numerical simulation. Moreover, a summary of literature on channel coding for PLS is provided.

The system and channel model for a MR geostationary SATCOM system is described in Chapter 3. Moreover, the scenario considered for the numerical simulations performed in this thesis is included. Multiple users and multiple eavesdroppers are located in the beam coverage of the exemplary scenario. Besides, the estimation of the CSI and basic ZF MU-MIMO precoding are introduced. ZF precoding will be a performance reference in the numerical simulations and demonstrates how much capacity must be sacrificed for security.

The minimum secrecy capacity precoding proposed in Chapter 4 is the first suitable metric for PLS in SATCOM. The goal is to generate a channel condition such that the legitimate users receive the signals in higher quality than all eavesdroppers and, thus,

fulfilling the requirement of key-less PLS. Since the minimum secrecy capacity (MSC) precoding algorithm is complicated to solve in the direct form, a reformulation to a convex form is provided to be solvable in polynomial time with off-the-shelf numerical programs. Numerical simulations proof the effectiveness of the algorithm and illustrate the security gains compared to the SR antenna design.

A second precoding for the more practically relevant security gap secrecy metric is proposed in Chapter 5. The security gap (SG) precoding leads to a specific gap between the received signal quality of the users and the eavesdroppers to, again, fulfilling the requirement of key-less PLS. After the reformulation of the nonconvex problem to a convex form, an iterative algorithm selects the best user signal quality achievable for the given positions of users and eavesdroppers. The effectiveness of achieving security and minimal losses in user signal quality are illustrated by numerical simulations.

1.5.2 Publications with Excerpts of this Thesis

- M. G. Schraml, R. T. Schwarz, and A. Knopp, "Multiuser MIMO Concept for Physical Layer Security in Multibeam Satellite Systems", *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1670–1680, 2021. DOI: 10.1109/TIFS.2020.3040884.

- M. G. Schraml and A. Knopp, "Precoding for Security Gap Physical Layer Security in Multiuser MIMO Satellite Systems", in *MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM)*, 2022, pp. 612–617. DOI: 10.1109/MILCOM55135.2022.10017639.

- M. G. Schraml, A. Knopp, and K.-U. Storek, "Multi-User MIMO Satellite Communications with Secrecy Constraints", in *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*, 2019, pp. 17–22. DOI: 10.1109/MILCOM47813.2019.9020847.

1.5.3 Publications Supporting this Thesis

- T. Delamotte, M. G. Schraml, R. T. Schwarz, K.-U. Storek, and A. Knopp, "Multi-Antenna-Enabled 6G Satellite Systems: Roadmap, Challenges and Opportunities", in *WSA 2021; 25th International ITG Workshop on Smart Antennas*, 2021, pp. 1–6.

- M. G. Schraml and A. Knopp, "Physical Layer Security with Unknown Eavesdroppers in Beyond-5G MU-MIMO SATCOM", in *2020 IEEE 3rd 5G World Forum (5GWF)*, 2020, pp. 180–185. DOI: 10.1109/5GWF49715.2020.9221107.

- S. P. Winter, M. G. Schraml, M. T. Knopp, and A. Knopp, "Spatial Modulation for Improved Eavesdropping Resistance in Multi-Beam Satellite Downlinks", in *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, 2018, pp. 829–834. DOI: 10.1109/MILCOM.2018.8599822.
- M. G. Schraml and A. Knopp, "Blind Estimation of the HPA Operating Point in Multicarrier Satellite Transponders", *IEEE Communications Letters*, vol. 21, no. 5, pp. 1051–1054, 2017. DOI: 10.1109/LCOMM.2017.2653118.
- M. G. Schraml and A. Knopp, "Cumulant based operating point estimation for communication satellite transponders", in *2017 IEEE International Conference on Communications (ICC)*, 2017, pp. 1–7. DOI: 10.1109/ICC.2017.7996646.

2 Physical Layer Security

This chapter starts with a differentiation of wireless physical layer security schemes. Physical layer security is commonly divided into key-less and key-based approaches [HFA19]. The key-based approach generates randomness based on the physical layer channel to encrypt the data before the transmission and is therefore called physical layer key generation (PLKG). The key-less approach is based on a higher channel quality, i.e. a higher SNR, from the transmitter to the intended receiver than to the eavesdropper. Nothing more than a wireless physical channel is necessary to achieve *perfect secrecy* [Wyn75]. In the following, PLS connotes the key-less approach and not the holistic concept of achieving security via physical layer features. The fundamentals of PLS are summarized in Section 2.1.3. Moreover, the authentication of a data transmission based on physical layer features is called physical layer authentication (PLA).

Fig. 2.1 shows the connection of this thesis to the big picture of physical layer security. PLS can be enabled by techniques like channel coding, the adaption of the channel, or the insertion of artificial signals in the time, frequency, or space domain [HFA19]. Moreover, an evaluation of the security performance of the algorithms is necessary. Secrecy metrics and their suitability for SATCOM are presented in Section 2.2. In this thesis, the goal is to construct channels which are suitable for key-less PLS, whereas the respective channel coding is not covered. The focus is on MU-MIMO precoding algorithms to achieve a high secrecy capacity in Chapter 4 and a high security gap in Chapter 5.

2.1 Differentiation: Wireless Security Schemes

To describe the wireless security scenarios, it makes sense to use the fictional characters which are common in cryptological literature. The pair of legitimate transmitter Alice and receiver Bob want to exchange secure messages or keys. They were first mentioned in [RSA78] to describe their public-key cryptosystem Rivest-Shamir-Adleman (RSA). The passive adversary Eve who knows everything about the transmission scheme used by Alice and Bob, i.e. is aware, tries to listen to the communication between Alice and Bob. The

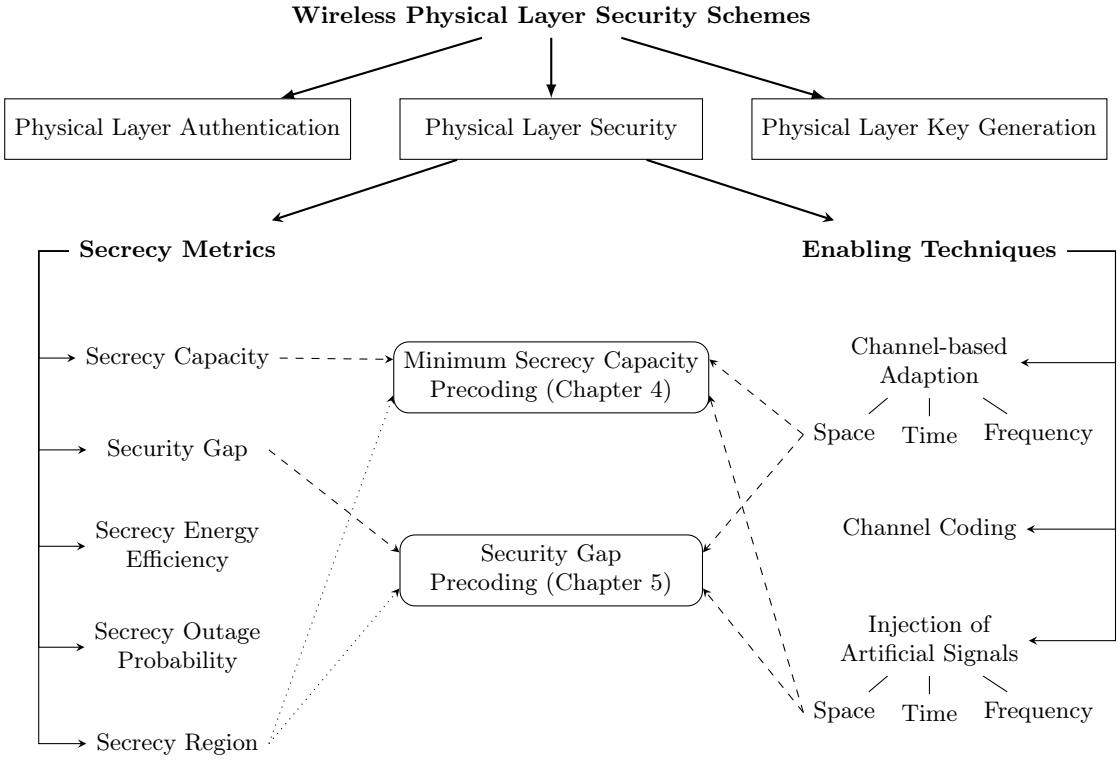

Figure 2.1: The big picture of Physical Layer Security and the connection to the precoding utilized in this thesis

malicious attacker Mallory can, additionally to Eve, also transmit messages for example to impersonate as Alice or replay messages from Alice to spoof Bob.

2.1.1 Physical Layer Authentication

One core concept of secure communications is to guarantee that the message actually comes from the legitimate source, namely Alice. This includes data integrity, data origin authentication, and sometimes also uniqueness and timeliness. A common method to provide these guarantees is multiplexing a message authentication code (MAC) to the message [MvOV97, Ch. 9 and 10]. Otherwise, Mallory can attack the communications system by modifying messages or transmit malicious messages. Even with MACs or encryption, Mallory can replay valid messages to spoof the receiver Bob. Timestamps, sequence numbers, or challenge-response protocols are some ways to fight replay attacks. Moreover, the MACs may leak information about the secret keys allowing for more advanced message forgery after Mallory has been able to recover the secret keys.

However, the multiplexed MACs need computational power for the cryptographic-based algorithms, reduce the data throughput, or increase the latency which might not be applicable in, for example, internet of things (IoT) devices or unmanned aerial vehicles (UAVs). PLA approaches are suitable candidates to overcome these drawbacks. Machine learning based algorithms for radio frequency fingerprinting, i.e. using physical layer features like carrier frequency offsets (CFOs), inphase-quadrature distortions, or channel impulse responses, can identify and authenticate different IoT devices [FWH19; MWM19]. Admittedly, these features are noisy and time-varying, so they can only assist in reliable authentication to prevent replay attacks. Superimposing a low power authentication signal, generated with a pre-shared key, with the message signal is a secure and bandwidth-efficient solution for message authentication [YVS15]. Additionally, this PLA scheme increases the key equivocation at Eve or Mallory, i.e. the protection of the secret keys.

The lack of authentication in global navigation satellite system (GNSS) signals allows for spoofing attacks to mislead the user with wrong positioning or timing information [WZY+20]. In contrast to jamming, i.e. denial-of-service attacks, it is difficult for the victims to detect the spoofing attacks and, thus, they are more harmful. Different strategies based on the physical layer characteristics of the GNSS signals are proposed in literature [WZY+20]. The propagation paths of the authentic GNSS signals are different for each satellite, whereas Mallory generally has to mimic signals of multiple satellites with a single transmitter. These differences can be used to detect fake GNSS signals [HBJL18; LW16]. Moreover, spoofing signals will interfere with the authentic signals and lead to significant distortions or high signal power at the receiver and enables the detection of spoofing and jamming attacks [WGHE18].

GNSS and IoT receivers typically use omnidirectional antennas which allow for easy spoofing with a transmitter located nearby on Earth. Contrarily, SATCOM systems have highly directional antennas, e.g. dish or phased array antennas, and potential spoofers must use UAVs or other satellites to transmit within the beam of the receiver. Thus, spoofing a SATCOM system is tremendously complicated and measures like Doppler frequency shift [FFWL21] or received signal strength (RSS) can be sufficient to authenticate the transmitter.

2.1.2 Physical Layer Key Generation

In many scenarios, Alice and Bob initially do not know each other and need to establish secure communications on the fly. Symmetric encryption schemes like advanced encryption standard (AES) [DBN+01] are usually employed for data protection thanks to their efficiency in data encryption. However, Alice and Bob need to share a common secret key

beforehand over an insecure channel which is commonly done with asymmetric encryption schemes, also known as public key cryptography. The Diffie-Hellman key exchange protocol [DH76] and its derivatives are widely used for Internet services today.

Public key cryptography is based on public and private key pairs where Alice encrypts a message with Bob's public key and Bob can decrypt the ciphertext with his private key. The security depends on the computational hardness of the inversion of some mathematical problems, for example the factorization of large numbers in RSA encryption [RSA78]. This computational security is fragile due to the rapid development of computer technology and future quantum computers [Sho97]. Additionally, it requires a key distribution infrastructure for the public keys which must be secured as well.

An alternative way to share a secret key between Alice and Bob is to exploit the uniqueness of wireless channels. This is called PLKG, in which the transceivers measure wireless channel characteristics and use them as shared random sources to generate a shared key [Zen15; ZDMW16]. The PLKG mechanisms relies on the physical laws of the wireless channels and are not dependent on the computational hardness of a mathematical problem. Therefore, the generated keys can achieve information-theoretic security which makes them candidates for quantum-proof key distribution schemes. The main communication between Alice and Bob is then performed with symmetric encryption schemes like AES which is quantum computing resistant, although larger key sizes are necessary [CJL+16].

Many PLKG mechanisms are based on, for example, RSS or CSI measures in non-line-of-sight time-division duplexing (TDD) systems [PDW19; FHA21]. In TDD systems where both the uplink and downlink are in the same carrier frequency band, the channel responses obtained by Alice and Bob are reciprocal. Practically, these measures are typically error-prone (with low probability) due to the noise and the fact that Alice and Bob cannot measure the channel at the same time in half-duplex communications. Moreover, Eve may have partial information about the common randomness. Hence, the measures cannot be used as a key for encryption directly. The authors of [Mau93] and [AC93] have shown that public discussion between Alice and Bob can still lead to secure keys. The process of PLKG is composed of the following steps: channel probing, randomness extraction, quantization, information reconciliation (correcting the errors), and privacy amplification (eliminating Eve's partial information) [Zen15].

For LOS SATCOM or spacecraft communications, Doppler frequency shift can be utilized to generate secret keys [TKY21]. If Alice and Bob are close together, the GNSS satellite-to-Earth channel is a source of common randomness for key generation [ZWZ+21]. However, in frequency-division duplexing (FDD) systems with different uplink and down-

link frequencies, Alice and Bob may experience different channel responses. The PLKG in FDD systems is still an open question with only few publications [ZLZ+22]. When uplink and downlink frequencies are close to each other, the reciprocity holds for direction of arrival measures [HN21].

2.1.3 Physical Layer Security

Shannon was the first to consider the problem of confidentially transferring information between the source and the sink [Sha49]. The main goal is to deliver a message U reliably from a sender (Alice) to a legitimate recipient (Bob), while keeping it a secret from an eavesdropper (Eve) receiving the same signal as Bob. U is therefore mapped to a codeword X^n using a stochastic encoder where n denotes the number of channel uses. Then, X^n is transmitted and Y_{B}^n and Y_{E}^n are received at Bob and Eve, respectively. A message U is transmitted with perfect secrecy if it is statistically independent of the signal Y_{E}^n received by Eve, i.e. the mutual information $\mathrm{I}(U; Y_{\mathrm{E}}^n) = 0$. Unfortunately, the transmission of a secret message requires sharing a secret key between the sender and the receiver whose length is at least equal to the length of the message itself. One-time pad cryptography is a well-known example of such a perfect secure system. This, in turn, severely limits the practical usefulness of such a perfect cryptographic system. In the wireless medium, however, the signal captured by Bob and Eve follows different paths and experience various distortions. Wyner showed that confidential communication in discrete memoryless wiretap channels (DMWCs) between legitimate users is possible without sharing a secret key if Eve's channel is a degraded version of Bob's channel [Wyn75]. Moreover, he gave an upper bound of the reliable transmission rates with secrecy: the secrecy capacity C_S. This marks the starting point of the research on PLS. Csiszar and Korner proposed a broadcast channel with confidential messages where Alice transmits a common message to Bob and Eve and a secret message intended for Bob only. The result is the generalized secrecy capacity

$$\begin{aligned} C_S &= \max_{p_X(x)} (\mathrm{I}(X^n; Y_{\mathrm{B}}^n) - \mathrm{I}(X^n; Y_{\mathrm{E}}^n)) \\ &\geq \max_{p_X(x)} \mathrm{I}(X^n; Y_{\mathrm{B}}^n) - \max_{p_X(x)} \mathrm{I}(X^n; Y_{\mathrm{E}}^n), \end{aligned} \tag{2.1}$$

where $p_X(x)$ is the probability mass function of the discrete variable X [CK78]. This indicates that the secrecy capacity is, in general, at least equal or higher than the difference of the user capacity and the eavesdropper capacity. The secrecy capacity is still positive as long as the main channel is less noisy than the eavesdropper's channel.

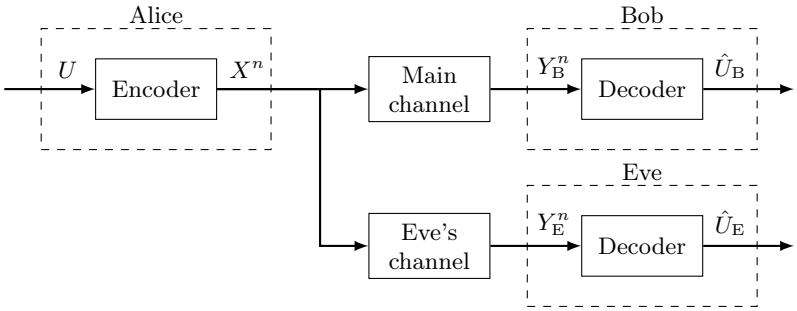

Figure 2.2: Generalized wiretap channel

The generalized wiretap channel by considering noisy communication channels is shown in Fig. 2.2. In [LH78] the special case of a wiretap channel with additive white Gaussian noise (AWGN), i.e. the Gaussian wiretap channel, is described. More recently, the secrecy capacity of other wireless channels is analyzed. The secrecy capacity in fading channels is characterized in [BD06] and [GLE08]. The extensions to multiple antennas and the MIMO channel are contributed by [OH08] and [KW10b], whereas the multiple-input single-output (MISO) channel is analyzed in [KW10a].

Besides the literature on PLS for FSS which has been presented in Section 1.5, the survey papers [AAE23] and [LFZZ20] provide insight into the topics of, for example, satellite-terrestrial integrated networks, satellite-terrestrial relay networks, and free space optical links. Moreover the LEO SATCOM is especially covered by [YAZ+22].

2.2 Secrecy Metrics and their Suitability for SATCOM

In the following, different secrecy metrics are provided. In order to evaluate and quantify the performance of a security scheme or algorithm, a suitable metric must be chosen which reflects how much secrecy can be provided by the proposed scheme. Especially, the suitability of the secrecy metrics for the MU-MIMO GEO SATCOM scenario is discussed.

2.2.1 Secrecy Capacity

In general, the capacity C_W is defined as the maximum data rate which can be transmitted quasi-error-free over the channel [Sha48]. Since algorithms for complex baseband signal processing are not bandwidth dependent, the signal bandwidth W can be normalized without loss of generality. The spectral efficiency C, measured in b/s/Hz, is the bandwidth-normalized channel capacity. Both metrics are used in the same manner for the rest of this thesis.

The secrecy capacity for wiretap channels with AWGN, i.e. Gaussian wiretap channels, is relevant for the GEO SATCOM scenario in this thesis. The secrecy capacity is given by

$$\begin{aligned} C_S &= C_\mathrm{B} - C_\mathrm{E} \\ &= \log_2(1+\gamma_\mathrm{B}) - \log_2(1+\gamma_\mathrm{E}), \end{aligned} \tag{2.2}$$

where γ_B and γ_E are the SNR value of the legitimate user and the eavesdropper, respectively [LH78][1]. The secrecy capacity is the upper bound of the data rate for secure communication R_S, i.e. $R_S < C_S$. Therefore, sometimes the secrecy capacity is defined to be nonnegative, i.e. $C_S = [C_\mathrm{B} - C_\mathrm{E}]^+$, where $[\,\cdot\,]^+ = \max(\,\cdot\,, 0)$. This is due to the fact, that any secrecy capacity $C_S \leq 0$ indicates that there is no possibility for secure transmission. In this thesis, negative secrecy capacities are allowed to demonstrate the capabilities of the eavesdroppers.

Hence, a high secrecy capacity should be the primary goal in the design process of a PLS communications systems to achieve a high data rate for secure communication. In literature on PLS for SATCOM, the secrecy capacity is one of the most important design criterions [LFZZ20]. Although channel codes to achieve (or approach) secrecy capacity for DMWCs can be practically implemented, e.g. [MV11; BHT15], it is difficult to construct such codes for Gaussian wiretap channels [LLBS14; DKA+21]. Recently, deep learning methods are applied to tackle the problem [FSW19; BLJJ20]. Moreover, a combination of classical low density parity check (LDPC) channel coding and hash functions is proposed in [VH19] to provide secrecy for finite-length transmissions in Gaussian wiretap channels.

Sum Secrecy Capacity versus Minimum Secrecy Capacity

The goal of a secure communications system is to guarantee secrecy for all its users. The metric of choice to measure the maximal data rate of information theoretically secure communications is the secrecy capacity. For multiuser systems, there are two common optimization objectives: the sum secrecy capacity, e.g. in [LAL19], and the minimum secrecy capacity, e.g. in [LLO+19]. However, from the user perspective, the sum secrecy capacity is not satisfactory since the solution is highly unfair. Considering two small examples with two users and a single eavesdropper in each case reveals that drawback:

1. First user's secrecy capacity 7.0 b/s/Hz + second user's secrecy capacity 0.0 b/s/Hz = sum secrecy capacity 7.0 b/s/Hz

[1] In [LH78], the factor 1/2 of the channel capacities is due to the real-valued AWGN channel. For complex-valued AWGN channels, this factor can be omitted [TV05].

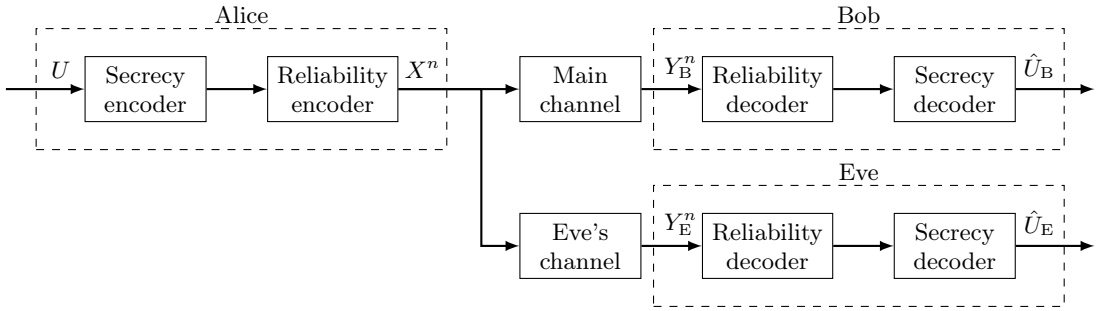

Figure 2.3: Multi-stage coding approach to secure communications.

2. First user's secrecy capacity 3.0 b/s/Hz + second user's secrecy capacity 3.0 b/s/Hz = sum secrecy capacity 6.0 b/s/Hz

The sum secrecy capacity objective will optimize for the first example since the sum secrecy capacity is higher. However, the second user is not able to transmit data securely due to a secrecy capacity of 0.0 b/s/Hz. Therefore, the objective of the system should be to achieve the highest secure data rate for all users, hence maximizing the minimum secrecy capacity. This is given in the second example where both users achieve a secrecy capacity of 3.0 b/s/Hz. For this reason, the minimum secrecy capacity is chosen as an optimization objective in this thesis.

2.2.2 Security Gap

For Gaussian wiretap channels, the BER over message bits is a more practical security metric [KHM+11; BBC12]. Recently, multi-stage approaches are proposed to achieve information-theoretic security over Gaussian wiretap channels [HFGV19; TMV+21]. With application of an inner error correction code (ECC) (reliability code), the transmissions between Alice and Bob as well as Alice and Eve see discrete memoryless channels. Moreover, the code achieves the reliability threshold at Bob, i.e. the channel is assumed to be quasi-noiseless. A state-of-the-art secrecy code, e.g. a Polar or LDPC code, is the outer code to guarantee information-theoretic security [MV11; BHT15]. The concept of the multi-stage approach is shown in Fig. 2.3.

With use of the inner ECC, Alice wants to reliably transmit a message to Bob which implies that the average BER p_e^{B} must be smaller than a predefined reliability threshold $p_{e,\max}^{\mathrm{B}}$. If the average BER of Eve p_e^{E} is close to 0.5 with i.i.d. errors, Eve is not able to extract useful information from the received messages. Hence, p_e^{E} should be higher than the security threshold $p_{e,\min}^{\mathrm{E}}$. For a specific ECC, these BER thresholds translate to certain SNR values at the receivers. SNR values above the reliability threshold $\gamma_{\mathrm{B},\min}$

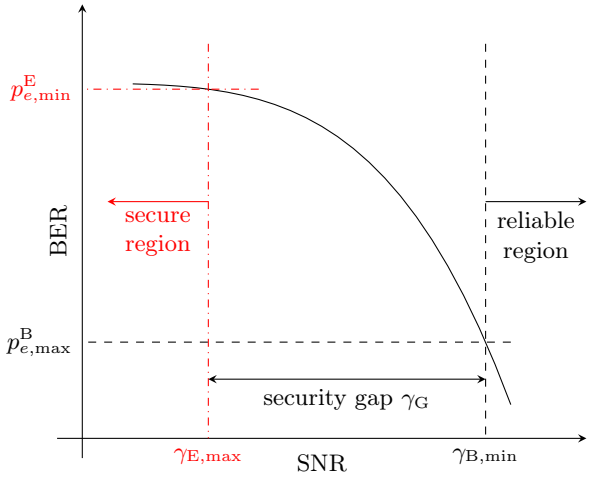

Figure 2.4: The BER over SNR performance curve of an ECC showing the security gap as well as the security and reliability regions.

lead to sufficiently low BERs, i.e. the condition $p_e^{\mathrm{B}} \leq p_{e,\max}^{\mathrm{B}}$ holds. Moreover, the security threshold $\gamma_{\mathrm{E,max}}$ is the highest SNR value for which $p_e^{\mathrm{E}} \geq p_{e,\min}^{\mathrm{E}}$ holds. SNR values below the security threshold are defined as security region and the ECC fails to decode almost every time. The outer channel is now highly degraded at Eve and secrecy codes can be applied.

The ratio $\gamma_{\mathrm{G}} = \gamma_{\mathrm{B,min}}/\gamma_{\mathrm{E,max}}$ is called security gap which is shown in Fig. 2.4. For PLS, ECCs which exhibit only a small security gap of a few decibel, i.e. with a steep waterfall region, are desired, for example punctured LDPC codes [KHM+11; PF22]. Moreover, bit-interleaved coded modulation can further reduce the security gap [MOS22]. Alice must shape the transmission signal into the direction of Bob to achieve a SNR difference between Bob and Eve. The performance of Eve's receiver is expected to be comparable to (or even better than) Bob's receiver performance. For a high probability that Eve's channel is inferior to the security threshold, the security gap should be as small as possible. Moreover, for system operators, the absolute value of $\gamma_{\mathrm{B,min}}$ is also important to select an adaptive coding and modulation (ACM) scheme to achieve the requested reliability. With feedback of Bob, the transmit power of Alice can be controlled to be close to the threshold not wasting signal power towards the eavesdroppers.

The DVB-S2X standard for SATCOM defines multiple ACM schemes, also called MODCODs. To achieve a low BER at the users, a reliability threshold $\gamma_{\mathrm{B,min}}$ must be achieved [DVBS2X, Ch. 6]. This is similar to the inner ECC of the multi-stage coding approach for PLS and, hence, the security gap metric fits well for SATCOM. This is why the security gap is also analyzed as a metric for optimization in this thesis.

2.2.3 Secrecy Energy Efficiency

The secrecy energy efficiency (SEE) is defined as the number of securely delivered bits per joule [NLS12]. The maximal achievable number of secure bits is given by the secrecy capacity in (2.2). Moreover, the power P_{T} which is necessary for transmission includes the signal power and the power consumption of all device electronics averaged over multiple timeslots or symbols. Hence, the SEE is given by $\eta_{\mathrm{SEE}} = C_S/P_{\mathrm{T}}$.

In times of climate protection and due to the limited power resources on a satellite, the SEE seems to be a promising metric. The authors of [LYO+19] maximize the SEE to serve a single earth station with a predefined SNR under secrecy constraints set for the eavesdroppers. However, SEE precoding under SNR constraints is similar to a power minimization. Hence, this metric is not considered in the thesis.

2.2.4 Secrecy Outage Probability

Alice knows the instantaneous CSI of Bob and, hence, the secrecy capacity of the channel. Both can agree on a code with the secrecy rate R_S. If the instantaneous secrecy capacity C_S is above that rate, the communication is secure. Due to a fading event of the channel, the instantaneous secrecy capacity C_S may drop below a target value R_S and the security of the system is compromised which is called secrecy outage [BD06]. The probability of such an event, the secrecy outage probability (SOP), is defined by

$$\Pr_{\mathrm{out}}(R_S) = \Pr(C_S < R_S) \tag{2.3}$$

The SOP metric is useful in situations where the instantaneous CSI of Eve is unknown but the fading characteristics of the channel are known at the transmitter. However, the SOP does not tell anything about the amount of information leakage to the eavesdroppers when outage occurs [HFA19]. Since the assumed SATCOM channel in the scenario of this thesis is AWGN without fading, the SOP metric is not further analyzed.

2.2.5 Secrecy Region

The secrecy region is defined as the geometrical area in which the secrecy capacity is above a certain threshold [MBH09]. The vulnerability region (VR), respectively, is the area where eavesdropping is possible, i.e. the secrecy capacity vanishes. If the eavesdropper locations are unknown, a system with a smaller VR can be seen as more secure. Instead of the SOP as a metric for short-time fading effects, the VR measures the security performance from the perspective of a large scale channel. As described in Chapter 3, the

channel for GEO SATCOM is approximately static. Hence, the secrecy region, and in the same way the VR, are in general well suited for GEO SATCOM. However, in this thesis, due to the large antennas which are necessary for eavesdropping, the eavesdropper location is assumed to be known. Therefore, the VR is not analyzed directly, but is part of Section 4.2.3 and Section 5.2.2 to demonstrate the effectiveness against new (potentially unknown) eavesdroppers.

3 Multiuser MIMO Satellite System and Channel Model

In this chapter, the basics of a MU-MIMO satellite link is thoroughly described. First, an overview of the system architecture is provided which includes the investigated scenario. A thorough description of the MU-MIMO downlink channel is presented which also includes the CSI estimation. Finally, the basics of MU-MIMO precoding are introduced with the example of ZF precoding.

3.1 Multiuser MIMO Satellite System Model

3.1.1 System Architecture

The forward link of a multiuser satellite system is considered in which a gateway station distributes K different sensitive data streams that are intended for K single-antenna user terminals (UTs). The GEO satellite employs a single feed per beam (SFPB) antenna architecture with L_{R} reflectors generating L user beams on Earth. The feeder link is considered to be ideal compared to the user downlink, i.e. noise contributions and distortions in the uplink can be neglected because the link budget is clearly limited by the downlink. Additionally, the uplink noise is a natural barrier for the achievable SNR which may prevent the assumption of highly advantaged eavesdroppers. An FFR scheme is assumed in the downlink. Hence, all beams use the same spectrum and polarization such that a MU-MIMO channel is formed between the L feeds and K users, where $L \geq K$. Moreover, there are M non-colluding eavesdroppers distributed in the coverage of all beams and try to intercept the sensitive data. It is assumed that the burden of receiver synchronization over hundreds of kilometers is also too high for the eavesdroppers. In Fig. 3.1, the multibeam SATCOM design with multiple users and eavesdroppers is illustrated. For clarity, only two out of L_{R} reflectors and the corresponding LOS paths to the kth user and mth eavesdropper are shown. The channel coefficients of the users $h_{\mathrm{B},kl}$

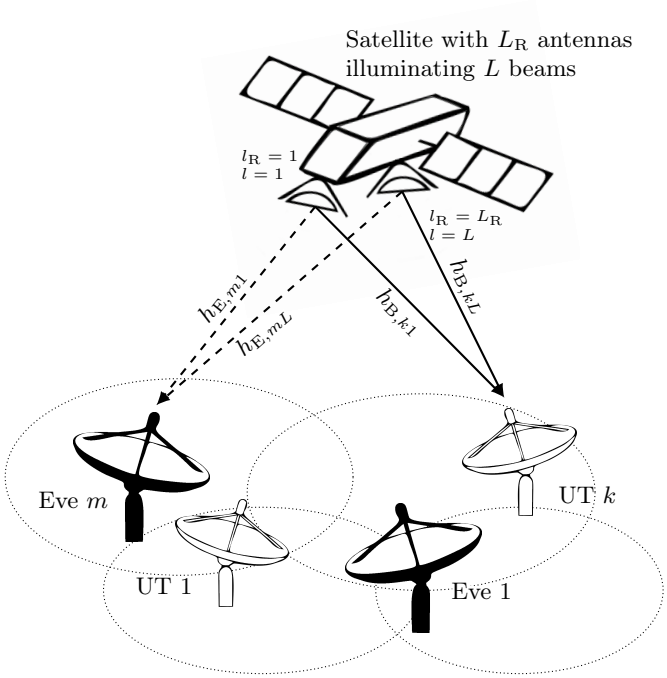

Figure 3.1: System model showing two users and two eavesdroppers in a multibeam SATCOM setup

and eavesdroppers $h_{\mathrm{E},ml}$, respectively, are described in detail in Section 3.2.

The satellite can employ, in general, any transparent or digital amplify-and-forward payload. An exemplary payload is shown in Fig. 3.2. The uplink to the satellite is exemplarily performed in a frequency-division multiple access (FDMA) scheme, but a MIMO feeder link is also possible [Del19]. Input multiplexer bandpass filters select each downlink beam signal which is converted to the same downlink carrier frequency. The high power amplifiers (HPAs) amplify the signals and bandpass filters remove out-of-band components generated due to the nonlinearity of the HPA [MBS20]. The satellite illuminates in total L beams with L_R reflectors based on an SFPB architecture, so that on average L/L_R beams are illuminated by the same reflector. The distance of the reflectors and the distance of the users on Earth must match the design rules in [Sch19] such that a MU-MIMO channel is formed. A multiple-reflector approach is already applied in a state-of-the-art satellite designs to improve the signal quality [FTA+16].

3.1.2 Scenario under Investigation

The scenario of a forward link of a single-satellite MU-MIMO HTS system is considered in this thesis. For reasons of readability of the results in the figures of this thesis, a 4×2

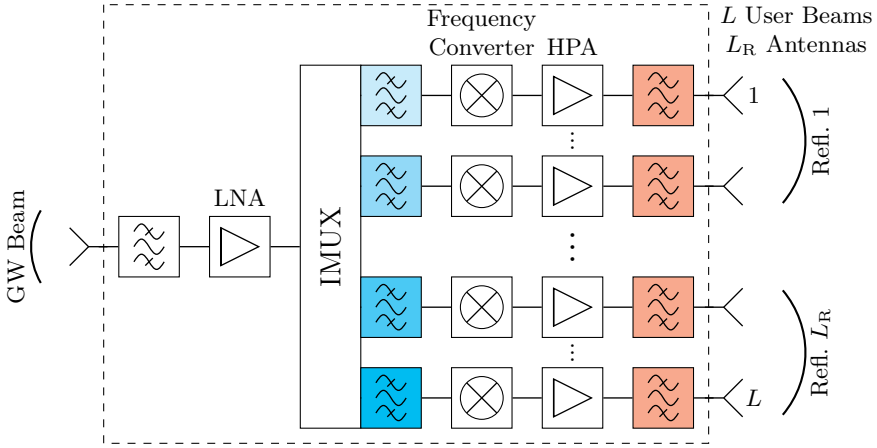

Figure 3.2: Block diagram of a transparent payload design for MU-MIMO downlinks

MU-MIMO setup is discussed as an example. However, this does not mean a restriction of the proposed algorithms to this particular antenna setup. The algorithms and the results can be easily scaled to support the general $L \times K$ MU-MIMO case.

The satellite illuminates $L = 4$ beams in Central Europe ranging from Poland to France in the east-west direction and from Denmark to Italy in north-south direction. The $-3\,\mathrm{dB}$ relative gain contour lines on Earth are shown in Fig. 3.3. An FFR scheme is applied where all beams share the same carrier frequency and a common polarization. In general, neighboring or overlapping beams are illuminated by spatially separated reflectors and, thus, $L_\mathrm{R} = 4$ in this MR scenario, i.e. each beam is illuminated by a separate reflector indicated by the numbers 1 to 4 in Fig. 3.3. The reflectors are geometrically arranged as a uniform circular array with a diameter D_S of 12 m. $M = 8$ eavesdroppers are shown in Fig. 3.3, whereas not all are active at the same time depending on the considered scenario. In case of $M = 2$, only E_1 and E_2 are actively eavesdropping and if $M = 4$, only E_1 up to E_4 are intercepting, respectively. It is assumed that all UTs are equal in performance and each eavesdropper receiver has a 6 dB higher gain-to-noise-temperature (G/T) than the receivers of the UTs.[1] It is assumed that an area with a radius of 3 km around each eavesdropper is free of users. Since eavesdroppers with such large antennas like those considered in this thesis are operated in, for example, large military facilities, this assumption seems reasonable. Moreover, the CSI of nearby receivers is approximately equal (cf. Section 3.3.3) and, hence, it would be impossible to differentiate between users and eavesdroppers. The eavesdroppers E_1 up to E_4 are located nearby the beam boresight

[1] This G/T advantage can be achieved, for example, with an eavesdropper antenna that is double the size of the UT antenna.

resulting in the highest antenna power gain (cf. Section 3.2.2.1). In other words, the intended receivers are clearly disadvantaged with respect to the eavesdroppers in terms of receiver SNR in this thesis. This is in contrast to [ZAO12] where the eavesdroppers are at least 15 % of the beam diameter away from the beam center and their receiver G/T is equal to the receiver G/T of the UTs. K_{T} total users are randomly distributed within the dashed area in Fig. 3.3. They are divided into K_{G} groups of $K = 2$ users in each group, whereas, in general, $K \leq L$ to serve the users simultaneously [SDSK19]. The number of users per group is limited to $K = 2$ such that all users can be served simultaneously and a spatial degree of freedom is left for security optimizations. For the numerical simulations in Chapter 4 and Chapter 5, $K_{\mathrm{T}} = 500$ total users with random locations are generated and divided into $K_{\mathrm{G}} = 250$ groups of $K = 2$ users in each group. The groups are composed by applying the multiple antenna downlink orthogonal clustering (MADOC) user grouping algorithm presented in Section 3.5. In general, for MU-MIMO communications every group size of $K \geq 2$ is eligible.[2] The system parameters that have been assumed throughout the thesis are summarized in Table 3.1.

For comparison, a SR variant of this scenario is considered where all beams are illuminated by the first reflector, i.e. $L_{\mathrm{R}} = 1$. This simulates the LOS channel without MIMO capabilities which is the common channel model in literature for PLS in FSS SATCOM. All the other system parameters from Table 3.1 are kept strictly equal to demonstrate the advantage of multiple reflectors on the satellite. However, the SR antenna design scenario is always explicitly stated in the caption of a figure, whereas otherwise the MR antenna design is the default.

Table 3.1: System Parameters

Parameter	**Value**
Orbit Position	9 °E
Carrier Frequency	11.0 GHz
Beam EIRP	59 dB W
Noise Bandwidth	500 MHz
UT Gain	44 dB ($\approx$ 2.4 m dish diameter)
UT Noise Temperature	280 K
UT G/T	19.5 dB/K
Eavesdropper G/T	25.5 dB/K

[2] The system is just a MISO system in case of $K = 1$.

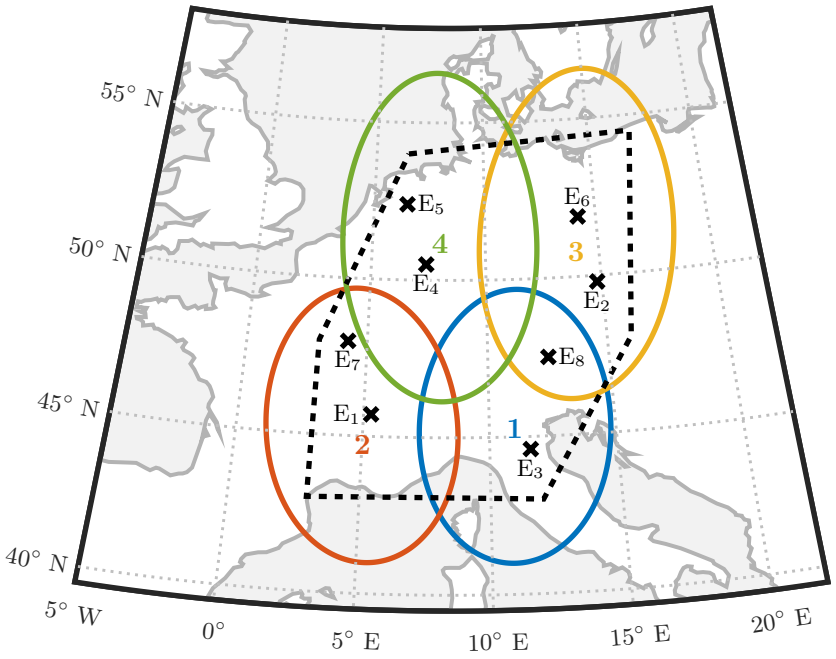

Figure 3.3: Scenario under investigation: The coverage zone in Central Europe is illuminated by $L = 4$ spot beams over $L_{\mathrm{R}} = 4$ reflectors. $M = 8$ eavesdroppers are distributed in the coverage zone and many users are randomly located within the dashed area.

3.1.3 Transmission Chain

The signals, channel coefficients and precoding vectors in this system model are time dependent. The discrete time representation of a signal with the sample period T_S and the time index $n \in \mathbb{Z}, -\infty \leq n \leq \infty$ is $x(t = nT_S) = x[n] = x$. For a more compact notation, the time index is omitted.

The data signal sent to the user is denoted by s_k, which is a zero mean complex random variable with unit variance ($\sigma_{s_k}^2 = 1$) generated by a capacity-achieving ACM scheme. This can be, for example, the common satellite transmission standard DVB-S2X [DVBS2X] or an ACM scheme with channel coding for PLS (cf. Chapter 2 and the reference therein). The data signals are mapped onto the antenna array with the precoding vectors $\mathbf{t}_k \in \mathbb{C}^{L \times 1}$ at the gateway station before transmission. This leads to the uplink signal to the lth feed of the satellite

$$x_l = \left[\sum_{k=1}^{K} \mathbf{t}_k s_k \right]_l , \tag{3.1}$$

whereas $[\,\cdot\,]_l$ denotes the lth element of the given vector. The vector $\mathbf{x} = [x_1, \ldots, x_L]^{\mathrm{T}}$ comprises all uplink signals. Since the feeder link is considered to be ideal, the uplink

signal to the satellite is equal to the signal transmitted by the satellite.

All channel propagation coefficients between the L feeds and the kth user receive antenna are defined by the column vector $\mathbf{h}_{\mathrm{B},k} = [h_{\mathrm{B},k1}, \ldots, h_{\mathrm{B},kL}]^{\mathrm{H}}$. The vector $\mathbf{h}_{\mathrm{B},k} \in \mathbb{C}^{L\times 1}$ is also called CSI of the kth user. The ray tracing of the spherical wave model is important to determine the channel propagation coefficients $h_{\mathrm{B},kl}$ which are defined in the Section 3.2. The received signal $y_{\mathrm{B},k}$ for user k is given by

$$\begin{aligned} y_{\mathrm{B},k} &= \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{x} + w_{\mathrm{B},k} \\ &= \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_k s_k + \sum_{i=1,i\neq k}^{K} \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_i s_i + w_{\mathrm{B},k}, \end{aligned} \tag{3.2}$$

with $w_{\mathrm{B},k}$ being the AWGN, which is complex circular symmetric with zero mean and variance $\sigma^2_{w_{\mathrm{B},k}}$. In multiuser systems, the interference caused by other users is typically treated as noise. To indicate the involved interference to the reader, γ_{B} is called signal-to-interference-plus-noise ratio (SINR) value of the user k and is given by

$$\gamma_{\mathrm{B},k} = \frac{\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_k\right|^2}{\sum_{i\neq k}\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_i\right|^2 + \sigma^2_{w_{\mathrm{B},k}}}. \tag{3.3}$$

Similar to the definition of the user channel vector, the vector $\mathbf{h}_{\mathrm{E},m} = [h_{\mathrm{E},m1}, \ldots, h_{\mathrm{E},mL}]^{\mathrm{H}}$ defines the channel vector of the mth eavesdropper containing the channel coefficients between the L feeds and the position of the mth eavesdropper receive antenna. The received signal $y_{\mathrm{E},mk}$ at the mth eavesdropper intending to intercept the kth user data stream is given by

$$y_{\mathrm{E},mk} = \mathbf{h}_{\mathrm{E},m}^{\mathrm{H}}\mathbf{t}_k s_k + \sum_{i=1,i\neq k}^{K} \mathbf{h}_{\mathrm{E},m}^{\mathrm{H}}\mathbf{t}_i s_i + w_{\mathrm{E},m}, \tag{3.4}$$

where the noise $w_{\mathrm{E},m}$ is complex circular symmetric with zero mean and variance $\sigma^2_{w_{\mathrm{E},m}}$. Since it is assumed that every eavesdropper is theoretically capable of wiretapping every user, i.e. synchronizing, demodulating and decoding the corresponding data stream of each user, K SINR values are defined for each eavesdropper. The mth eavesdropper can receive the kth user signal with the SINR

$$\gamma_{\mathrm{E},mk} = \frac{\left|\mathbf{h}_{\mathrm{E},m}^{\mathrm{H}}\mathbf{t}_k\right|^2}{\sum_{i\neq k}\left|\mathbf{h}_{\mathrm{E},m}^{\mathrm{H}}\mathbf{t}_i\right|^2 + \sigma^2_{w_{\mathrm{E},m}}}. \tag{3.5}$$

In practice, only the highest SINR value per eavesdropper is relevant. If one can decode the first user signal, successive interference cancellation (SIC) can be applied to improve the SINR to wiretap the other users.

Moreover, AN is helpful to increase the security of a system [GN08]. The artificial noise a is a zero mean complex circular symmetric Gaussian random variable with unit variance. The AN signal is mapped onto the antenna array with the precoding vector $\mathbf{t}_a \in \mathbb{C}^{L\times 1}$, respectively. The simple method is to lay the AN in the null space of the user signal to avoid interference, which, however, limits the degrees of freedom during the optimization process. Therefore, the general case is considered where interference between the user signal and AN is allowed but may deteriorate the user SINR. The received signal at the kth UT is given by

$$y_{\mathrm{B},k} = \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_k s_k + \sum_{i=1,i\neq k}^{K} \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_i s_i + \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_a a + w_{\mathrm{B},k}, \tag{3.6}$$

This leads to the respective SINR of the kth user with AN:

$$\gamma_{\mathrm{B},k}^{\mathrm{AN}} = \frac{\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_k\right|^2}{\sum_{i\neq k}\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_i\right|^2 + \left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_a\right|^2 + \sigma_{w_{\mathrm{B},k}}^2}. \tag{3.7}$$

The AN is received by the eavesdroppers as well and deteriorates their SINRs which are in that case given by

$$\gamma_{\mathrm{E},mk}^{\mathrm{AN}} = \frac{\left|\mathbf{h}_{\mathrm{E},m}^{\mathrm{H}}\mathbf{t}_k\right|^2}{\sum_{i\neq k}\left|\mathbf{h}_{\mathrm{E},m}^{\mathrm{H}}\mathbf{t}_i\right|^2 + \left|\mathbf{h}_{\mathrm{E},m}^{\mathrm{H}}\mathbf{t}_a\right|^2 + \sigma_{w_{\mathrm{E},m}}^2}. \tag{3.8}$$

3.2 Multiuser MIMO Satellite Channel Model

The channel propagation coefficients contain the whole link-budget of the transmission. Therefore, three main components of the coefficients are considered:

1. the feeder link, the power amplifiers and the frequency converters which are only dependent on the beam index l,

2. the satellite transmit antenna gain and the free space propagation (FSP) which are influenced by the beam index l and the position of the user and eavesdropper terminals,

3. the gain and phase of the receiver earth stations for users and eavesdroppers, respectively, which are independent of the MU-MIMO setup.

Although the channel model is presented for the user channel coefficient $h_{\mathrm{B},kl}$ in the following, it can be derived equivalently for the eavesdropper channel coefficient $h_{\mathrm{E},ml}$ by replacing the respective indices.

3.2.1 Uplink to the Satellite and the Transponders

The feeder link and satellite transponder of the lth downlink beam is a single-input single-output (SISO) channel due to the FDMA scheme. The gain $g_l^{\mathrm{UL}} \in \mathbb{C}$ models the uplink channel of the lth beam:

$$g_l^{\mathrm{UL}} = a_l^{\mathrm{UL}} \, \mathrm{e}^{\mathrm{j}\varphi_l^{\mathrm{UL}}} . \tag{3.9}$$

The power gain $a_l^{\mathrm{UL}} \in \mathbb{R}$ comprises the gateway equivalent isotropically radiated power, the uplink FSP loss, the satellite receive antenna gain, the depointing losses, as well as the gains and losses of the satellite payload, e.g. the low noise amplifier, HPA and bandpass filters. The phase $\varphi_l^{\mathrm{UL}} \in [-\pi, \pi[$ is influenced by the gateway local oscillator (LO), the varying path length towards the satellite and the phase shift in the payload components. From the downlink perspective, g_l^{UL}, $1 \leq l \leq L$, affects all users and eavesdroppers in the same way. The power $a_l^{\mathrm{UL}} = a^{\mathrm{UL}}$ can be assumed to be constant due to the fact that satellite operators measure the output backoff of the HPAs and are able to adjust the output power to be equal for all beams [SK17a]. This can be done by adjusting the uplink power accordingly. However, the φ_l^{UL} in (3.9) must be considered to achieve effective precoding.

3.2.2 Downlink Propagation

3.2.2.1 Antenna Radiation Pattern

It has been shown in [SDSK19] and the references therein that, for frequencies above 10 GHz and in case of directional antennas, it is sufficient to take only the LOS FSP as well as the multibeam antenna pattern into account to model the channel propagation coefficients. The antenna boresight is the direction of the antenna's main lobe for which the power is maximum and points towards the beam center position on Earth. Hence, the transmit antenna gain depends on the pattern of the multibeam antenna and the position of the user or eavesdropper within the illuminated beam. In the following, $\lambda_c = \mathrm{c}_0/f_c$ denotes the carrier wavelength with c_0 and f_c being the speed of light and the carrier

frequency, respectively. The angle θ_{kl} denotes the off-axis angle of the kth Earth terminal with respect to the lth beam's boresight direction based on the position of the utilized reflector $\mathbf{r}_{l_\mathrm{R}}$. Parameter $a^\mathrm{R}_{l,\max}$ denotes the maximal power gain of the satellite transmit reflector with diameter D_{l_R} used to illuminate the lth beam. The satellite antenna gain $a^\mathrm{R}_{kl} \in \mathbb{R}$ is modeled by [ST12]:

$$a^\mathrm{R}_{kl} = a^\mathrm{R}_{\max} \left(\frac{J_1(u)}{2u} + 36 \frac{J_3(u)}{u^3} \right), \tag{3.10}$$

where $u = \pi D_{l_\mathrm{R}} / \lambda_c \cdot \sin(\theta_{kl})$, and $J_1(\,\cdot\,), J_3(\,\cdot\,)$ are Bessel functions of the first kind and order one and three, respectively.

3.2.2.2 Free Space Path Loss

The radio radio path length between the kth user and the lth satellite feed is denoted by $d_{kl} = \|\mathbf{r}_l - \mathbf{r}_k\|$. Moreover, the radio path length between the lth feed and the reflector l_R is static and equal for all users and eavesdroppers. Hence, it can be omitted which reduces the relevant radio path length to the distance between the satellite reflector l_R and the UT antenna. The FSP gain g^FSP_{kl} between the beam l and user k is then given by

$$g^\mathrm{FSP}_{kl} = \frac{\lambda_c}{4\pi d_{kl}} \cdot \mathrm{e}^{-\mathrm{j}\frac{2\pi}{\lambda_c} d_{kl}}. \tag{3.11}$$

Besides the FSP loss, the atmospheric distortions must be considered. For SATCOM and frequencies above 10 GHz, the troposphere (from ground up to 20 km altitude) is most significant [All11]. An antenna separation of a few meters on the satellite and a maximum altitude of severe weather influences at 20 km, result in a horizontal separation of the LOS paths of only a few centimeters [Sch19]. Hence, it is reasonable to assume identical amplitude and phase disturbances in the troposphere for all paths from different satellite antennas to the same UT. To investigate potential phase fluctuations between different LOS radio paths due to atmospheric perturbations, various interferometric measurements in radio astronomy and SATCOM have been conducted (see [SHK15a] and references therein). The measurement results have shown that the root mean square differences of the radio path length due to atmospheric influences is below 190 µm (2.8° at 12.5 GHz carrier frequency) in 99% of all observations [SHK15b]. It is, therefore, sufficient to consider the deterministically calculated phase of the pure LOS path via ray tracing in a spherical wave model. The phase fluctuations that are potentially induced by the atmosphere can be neglected in this model.

3.2.3 Modeling the Receiver Terminals

The model of the receiver terminal also includes the remaining severe weather influences in the troposphere, for example, the rain attenuation. This is due to the fact that they affect each UT separately. The kth UT consists of an antenna and a down converter. Their total gain g_k^{UT} is modeled by

$$g_k^{\mathrm{UT}} = a_k^{\mathrm{UT}} \, \mathrm{e}^{\mathrm{j}\varphi_k^{\mathrm{UT}}} \, . \tag{3.12}$$

An active antenna steering is considered to mitigate the depointing loss for all terminals, users and eavesdroppers, as this is a standard feature of large parabolic reflector antennas [MBS20]. If a user or eavesdropper uses a different receiver, e.g. a larger antenna or a down converter of better quality, or is affected by position dependent rain attenuation, its gain a_k^{UT} varies. Since an eavesdropper is negatively affected by rain attenuation, clear sky conditions as the worst case are assumed throughout this thesis. The φ_k^{UT} includes, for example, the LO of the down converter in the UT and the phase shift due to atmospheric perturbations which affects all radio paths equally.

3.2.4 Summary

The channel propagation coefficients $h_{\mathrm{B},kl}$ combining all introduced effects are finally given by

$$h_{\mathrm{B},kl} = a^{\mathrm{UL}} \, \mathrm{e}^{\mathrm{j}\varphi_l^{\mathrm{UL}}} \cdot a_{kl}^{\mathrm{R}} \cdot g_{kl}^{\mathrm{FSP}} \cdot a_k^{\mathrm{UT}} \, \mathrm{e}^{\mathrm{j}\varphi_k^{\mathrm{UT}}} \, . \tag{3.13}$$

The UT phase φ_k^{UT} is constant for all beams. It is recovered by the receiver and, thus, could be removed without loss of generality.

3.3 Channel State Information

3.3.1 User CSI with Feedback

The estimation of the CSI is crucial to perform the precoding. An UT can estimate its channel propagation coefficients at the same time with cross correlation of orthogonal training sequences transmitted in each beam. Possible sequences are based on constant amplitude zero autocorrelation waveform [HSSK16] or Walsh-Hadamard codewords [DVBS2X, Annex E]. The CSI of the users is known at the transmitter or gateway based on a feedback of the channel coefficients via a separate return channel. The update rate of the coefficients can be low (in the order of multiple seconds) due to the fact that the channel

is only slowly varying. In a testbed and field trial of a MU-MIMO SATCOM downlink scenario, the CSI update period of 5 s has shown to be sufficient to achieve the throughput predicted by theory [SSK20]. Since the testbed considered a MU-MIMO SATCOM setup with two collocated satellites, the CFOs due to the motion of the satellites have been tracked and compensated at the transmitting gateway additionally. For the single-satellite scenario considered in this thesis, the necessity of a CFO compensation depends on the uplink. A large uplink carrier frequency difference due to the considered FDMA scheme, e.g. using different frequency bands, possibly requires a CFO compensation.

3.3.2 CSI Estimation for Eavesdroppers

The eavesdroppers, however, do not feed back their channel propagation coefficients. With the assumption of an approximately known position of the mth eavesdropper $\mathbf{r}_m$ the derivation of the CSI starts. The position can be approximated by, for example, detection on satellite images or other intelligence services.

To estimate the antenna radiation pattern gain (3.10) and FSP gain (3.11) parts of the channel propagation coefficients, the position of the satellite feeds $\mathbf{r}_l$ are necessary. The stabilization of the yaw, roll and pitch axes of a satellite is done with high precision [MBS20]. Hence, there is a constant offset between all feed positions $\mathbf{r}_l$ and the center of mass of the satellite and the beam boresight positions are kept constant. The satellite position can be estimated with time difference of arrival measurements of four UTs [HX04]. Ray tracing algorithms can now compute the downlink propagation channel gains a_{ml}^{R} and g_{ml}^{FSP} for each position on Earth.

The uplink φ_l^{UL} for each beam cannot be estimated directly. However, the difference of the arguments of the coefficient measurement and the FSP gain result in

$$\varphi_l^{\mathrm{UL}} + \varphi_k^{\mathrm{UT}} = \arg(h_{\mathrm{B},kl}) - \arg\big(g_{kl}^{\mathrm{FSP}}\big). \tag{3.14}$$

Moreover, the phase of the UT can be eliminated by

$$(\varphi_l^{\mathrm{UL}} + \varphi_k^{\mathrm{UT}}) - (\varphi_1^{\mathrm{UL}} + \varphi_k^{\mathrm{UT}}) = \varphi_l^{\mathrm{UL}} - \varphi_1^{\mathrm{UL}} \tag{3.15}$$

which reveals the phase difference between the first and lth beam. The uplink phase

vector with the unknown offset φ_1^{UL} is given by

$$\boldsymbol{\varphi}^{\mathrm{UL}} = \begin{bmatrix} 0 \\ \varphi_2^{\mathrm{UL}} - \varphi_1^{\mathrm{UL}} \\ \vdots \\ \varphi_l^{\mathrm{UL}} - \varphi_1^{\mathrm{UL}} \end{bmatrix} + \varphi_1^{\mathrm{UL}} \tag{3.16}$$

The phase offset is not crucial for the CSI estimation, can be interpreted as a shifted UT LO phase as well, and will be recovered by the receivers anyway. If a single user is not able to receive the signals of all beams, multiple users with overlapping beam coverage are necessary to construct the vector $\boldsymbol{\varphi}^{\mathrm{UL}}$.

A defensive estimation of $|h_{\mathrm{E},ml}|$ can be done by assuming a best-in-class receiver and the parabolic reflector size on the pictures of the eavesdropper's position. In conclusion, the CSI of the eavesdropper $\mathbf{h}_{\mathrm{E},m}$ can be estimated with knowledge of the position $\mathbf{r}_m$ and multiple (at least four) reference users.

3.3.3 CSI Estimation Error

To demonstrate the channel propagation coefficient estimation error in dependency of a position error, it is assumed that the position error of the eavesdropper is in the order of a few kilometers. Hence, the amplitude variation of the channel coefficients can be neglected since the weather and the satellite antenna radiation gain can be assumed to be equal in such an area. Thus, the crucial part of the channel vector is the phase which is given by

$$\arg(\mathbf{h}_{\mathrm{E},m}) = \begin{bmatrix} \varphi_1 \\ \vdots \\ \varphi_L \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ \varphi_L - \varphi_1 \end{bmatrix} + \varphi_1. \tag{3.17}$$

Again, the constant offset φ_1 is irrelevant for the CSI since it can be recovered by the receiver. In case of a position error, this phases will be affected by errors:

$$\begin{aligned} \arg\left(\hat{\mathbf{h}}_{\mathrm{E},m}\right) &= \begin{bmatrix} 0 \\ \vdots \\ \varphi_L + \Delta\varphi_L - (\varphi_1 + \Delta\varphi_1) \end{bmatrix} + (\varphi_1 + \Delta\varphi_1) \\ &= \begin{bmatrix} 0 \\ \vdots \\ \varphi_L - \varphi_1 + (\Delta\varphi_L - \Delta\varphi_1) \end{bmatrix} + (\varphi_1 + \Delta\varphi_1). \end{aligned} \tag{3.18}$$

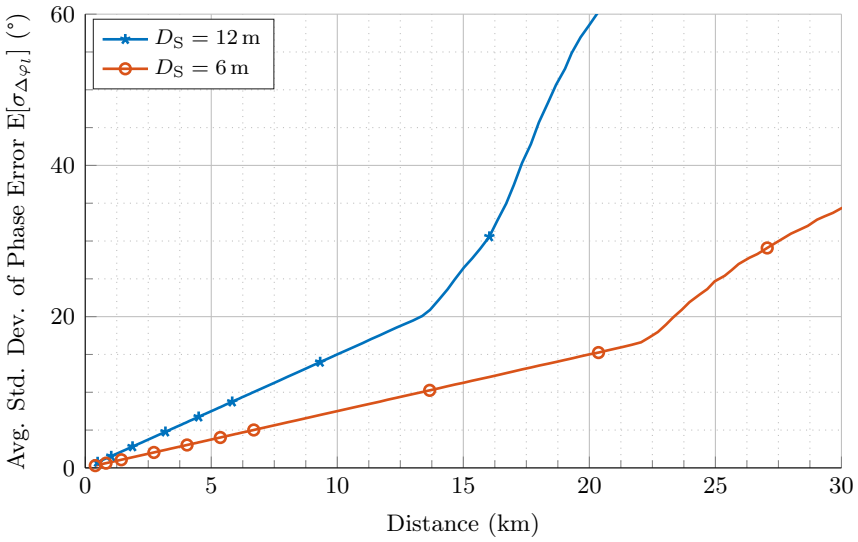

Figure 3.4: Standard deviation of the phase error in the CSI in dependency of the distance to the true position

The error of the first beam is randomly distributed, i.e. $\Delta\varphi_1 \in [-\pi, \pi[$. However, the relevant error terms are $(\Delta\varphi_l - \Delta\varphi_1)$ with their standard deviation $\sigma_{\Delta\varphi_l}$. A simulation with 1 000 000 equally distributed positions in a radius of 30 km around the true position with random altitudes between 0 m and 1000 m is performed. The average over all beams of the standard deviation of the phase error in dependency of the position error for different antenna spacings D_S on the satellite are shown in Fig. 3.4. The results are in line with the theory in [Sch19] that a larger spacing of the antennas on the satellite D_S leads to orthogonal channels when the antennas are closer together on Earth. A distance of a few meters in space still requires multiple kilometers of antenna spacing on Earth. With the larger spacing of $D_S = 12\,m$, the CSI variance of eavesdroppers and users close to each other is higher than the CSI variance with $D_S = 6\,m$. This is an advantage for secure MU-MIMO SATCOM precoding, but a drawback for the CSI estimation. However, for $D_S = 12\,m$, the CSI error due to position uncertainty of up to 3 km is in the order of the phase uncertainty after CFO compensation in [SSK20]. This error is sufficiently small such that MU-MIMO precoding becomes possible. Since the location of the eavesdroppers will be known more precisely than 3 km due to the precision of contemporary satellite imagery, it is assumed throughout this thesis to know the CSI of the eavesdroppers exactly.

In case of the SR variant, the eavesdroppers are not affected by the channel phase variations of the FSP loss in (3.11) dependent on the reflector position and terminal

position on Earth. The multibeam antenna pattern in (3.10) is the only degree of freedom and, hence, the CSI of the eavesdroppers is also perfectly known.

3.4 Introduction to Multiuser MIMO Precoding

3.4.1 Zero-Forcing Precoding

One of the common precoding algorithms for (multiuser) MIMO is ZF precoding [SSH04; YG06; WES08]. The precoding algorithm cancels out the co-channel interference (CCI) part for the other users in (3.19c), forces the interference to zero (hence the name). Two different objectives for optimization of each users signal power P_k are possible:

- Fairness: $f(P_k) = \min_k P_k$
- Throughput: $f(P_k) = \sum_k \log(1 + P_k)$.

While designing the ZF precoding vectors, for SATCOM an important practical aspect has to be considered: Every satellite feed has a dedicated power amplifier which prohibits an instantaneous power sharing between the L feeds, i.e. the per-antenna power constraint (PAPC) (3.19d) has to be considered. Since the channel vectors $\mathbf{h}_{\mathrm{B},k}$, including the channel propagation coefficients defined in (3.13), already include the physical signal power, the PAPC is bounded to 1. Moreover, the precoding algorithm must consider all users equally to mitigate CCI and, hence, the set of precoding vectors $(\mathbf{t}_1, \ldots, \mathbf{t}_K)$ must be optimized in a single step. The complete ZF precoding algorithm subject to the zero-interference constraint and the PAPC for SATCOM is given by:

$$\max_{(\mathbf{t}_1,\ldots,\mathbf{t}_K)} \quad f(P_k) \tag{3.19a}$$

$$\text{subject to} \quad \left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_k\right|^2 = P_k, \qquad \forall k, \tag{3.19b}$$

$$\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_i\right|^2 = 0, \qquad \forall i \neq k, \tag{3.19c}$$

$$\left[\sum_{k=1}^{K} \mathbf{t}_k \mathbf{t}_k^{\mathrm{H}}\right]_{l,l} \leq 1, \quad \forall l. \tag{3.19d}$$

The ZF precoding is used as a reference for performance in the latter of this work. Comparing the user capacity or SINR achieved by ZF with the respective values of the precodings for security, the performance scarified for security is revealed. A common method to reformulate the optimization problem to apply an computationally efficient numerical solving algorithm is introduced in the following Section 3.4.2.

3.4.2 Solving the Optimization Problem

The optimization problem (3.19) can be reformulated to be convex and, thus, efficiently solved with off-the-shelf numerical optimization methods. To be more precise, the optimization problem must follow the disciplined convex programming (DCP) rules [GBY06; BV04]. Exemplarily, CVX is a package for specifying and solving convex programs [GB08; GB20]. The ZF precoding with fairness objective can be reformulated to a second order cone program [WES08]. The throughput objective is more difficult and a more general convex reformulation, the semidefinite relaxation (SDR), is necessary [WES08]. In the following, the throughput objective is shown because of the necessity of the SDR reformulation for the secure precoding algorithms in Chapter 4 and Chapter 5.

In a first step, the quadratic terms must be linearized. The absolute square can be expressed by $\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_k\right|^2 = \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_k\mathbf{t}_k^{\mathrm{H}}\mathbf{h}_{\mathrm{B},k}$. Moreover, a matrix $\mathbf{T}_k = \mathbf{t}_k\mathbf{t}_k^{\mathrm{H}} \in \mathbb{C}^{L\times L}$ is defined. Due to the construction, this matrix is positive semidefinite, i.e. $\mathbf{T}_k \succeq 0$, and $\mathrm{rank}(\mathbf{T}_k) = 1$. The reformulation of (3.19) is given by:

$$
\begin{aligned}
\max_{(\mathbf{t}_1,\ldots,\mathbf{t}_K)} \quad & \sum_k \log(1+P_k) && && \text{(3.20a)}\\
\text{subject to} \quad & \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{T}_k\mathbf{h}_{\mathrm{B},k} = P_k, && \forall k, && \text{(3.20b)}\\
& \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{T}_i\mathbf{h}_{\mathrm{B},k} = 0, && \forall i \neq k, && \text{(3.20c)}\\
& \left[\sum_{k=1}^{K}\mathbf{T}_k\right]_{l,l} \leq 1, && \forall l, && \text{(3.20d)}\\
& \mathbf{T}_k \succeq 0, && \forall k, && \text{(3.20e)}\\
& \mathrm{rank}(\mathbf{T}_k) = 1, && \forall k. && \text{(3.20f)}
\end{aligned}
$$

However, this rank-one constraint (3.20f) is the only non-convex constraint in (3.20) and must be removed for efficient numerical optimization. The constraint on the positive semidefinite matrix is relaxed and, therefore, the procedure is called SDR [LMS+10]. The problem formulation which now follows the DCP rules is expressed as an instance of

semidefinite programming (SDP):

$$\begin{aligned} \max_{(\mathbf{T}_1,\ldots,\mathbf{T}_K)} \quad & \sum_k \log(1+\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{T}_k\mathbf{h}_{\mathrm{B},k}) \\ \text{subject to} \quad & \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{T}_i\mathbf{h}_{\mathrm{B},k} = 0, && \forall i \neq k, \\ & \left[\sum_{k=1}^{K}\mathbf{T}_k\right]_{l,l} \leq 1, && \forall l, \\ & \mathbf{T}_k \succeq 0, && \forall k. \end{aligned} \tag{3.21}$$

In particular, the original problem (3.19) with the throughput objective belongs to the class of NP-hard problem. The SDP problem (3.21) can be solved with interior-point algorithms in polynomial time with a worst-case complexity of

$$\mathcal{O}\Big(\sqrt{N_{\mathrm{Var}}}\big(N_{\mathrm{Cons}}N_{\mathrm{Var}}^2 + N_{\mathrm{Cons}}^{\omega} + N_{\mathrm{Var}}^{\omega}\big)\log(1/\epsilon)\Big) \tag{3.22}$$

given a solution accuracy $\epsilon > 0$ [JKL+20]. N_{Var} denotes the number of optimization variables, N_{Cons} the number of constraints and ω the complexity of a matrix inversion which is currently $\omega = 2.373$ [JKL+20].

Numerically solving (3.21) results in the globally optimal matrices $\mathbf{T}_k^*$ [LMS+10]. However, turning the NP-hard problem into a polynomial-time solvable problem, there is a fundamental issue of turning back the $\mathbf{T}_k^*$ into a feasible solution $\mathbf{t}_k^*$. The corresponding precoding vector $\mathbf{t}_k^*$ can be easily recovered by an eigendecomposition or singular value decomposition (SVD) if the optimal matrices are rank-one[3]. The eigenvector corresponding to the only nonzero eigenvalue is the optimal precoding vector $\mathbf{t}_k^*$. For the ZF precoding optimization problem, the SDR solution is always rank-one [WES08].

In general, it depends on the number of constraints if there is always a rank-one solution [HP10]. If these matrices $\mathbf{T}_k^*$ are a high rank optimal solution, there are many reasonable heuristics to determine an approximate solution $\mathbf{t}_k^{\circledast}$. In general, the result is not optimal. Otherwise, an NP-hard problem would have been solved in polynomial time [LMS+10]. In this work, the Gaussian randomization procedure is applied which is described in Fig. 3.5. The diagonal elements of $\mathbf{T}_k^*$ represent the optimal power of the user signal transmitted via the respective beam and, thus, the random vector is scaled accordingly.

[3]Numerically determining the rank of a matrix is done by an SVD and counting the singular values above a certain threshold $\epsilon > 0$. The resulting rank of the matrix is called ϵ-numerical rank.

Data: High rank optimal $\mathbf{T}_k^*$
Number of randomization iterations $I_{\max}$
Result: Suboptimal precoding vector $\mathbf{t}_k^{\circledast}$
for $i = 1, \ldots, I_{\max}$ **do**
Generate $\boldsymbol{\xi}_k^{(i)} \sim \mathcal{CN}(0, \mathbf{I}_L)$
Scale $\boldsymbol{\xi}_k^{(i)}$ such that $\left|\boldsymbol{\xi}_k^{(i)}\right|^2 = \operatorname{diag}(\mathbf{T}_k^*)$
end
Determine $i^{\circledast}$ which solves the original problem (3.19) the best
Output $\mathbf{t}_k^{\circledast} = \boldsymbol{\xi}_k^{(i^{\circledast})}$ as the approximate SDR solution

Figure 3.5: Gaussian randomization procedure to recover $\mathbf{t}_k^{\circledast}$.

3.5 User Selection for Precoding

Since the total number of potential users on Earth K_{T} is typically larger than the number of transmit antennas (beams) on the satellite, user scheduling is necessary. In order to serve every UT, all K_{T} UTs are divided into K_{G} groups, whereas the K UTs in the same group are served simultaneously with space division multiple access. Moreover, different groups can be served sequentially in different time slots in a time-division multiple access manner.

The algorithm proposed in [CQ19] iteratively adds new users to the group and tests the sum rate after precoding. Only users which contribute positively to the sum rate stay in the group. In [LZT+22], a genetic algorithm is presented where many populations of randomly grouped users are generated. After computing the precoding, the most powerful populations, i.e. the ones with the highest average data rate, are selected as parents. Randomly exchanging users of different groups forms the new generation. After a maximum number of generation, the algorithm terminates.

However, the computation of the precoding during the user grouping process might be feasible for ZF precoding but not for more complex ones like the security precoding algorithm proposed in Chapter 4. Therefore, the MADOC user grouping algorithm proposed in [SK17c] with the cosine similarity metric

$$\cos(\angle(\mathbf{h}_{\mathrm{B},i}, \mathbf{h}_{\mathrm{B},j})) = \frac{\left|\mathbf{h}_{\mathrm{B},i}^{\mathrm{H}} \mathbf{h}_{\mathrm{B},j}\right|}{\|\mathbf{h}_{\mathrm{B},i}\| \|\mathbf{h}_{\mathrm{B},j}\|} \tag{3.23}$$

is considered for the remainder of this thesis. The channel vectors $\mathbf{h}_{\mathrm{B},i}$ and $\mathbf{h}_{\mathrm{B},j}$ are orthogonal when $\cos(\angle(\mathbf{h}_{\mathrm{B},i}, \mathbf{h}_{\mathrm{B},j})) = 0$ which implies that user i and user j do not influence each other. Hence, a new user is added to the group when its cosine similarity (3.23) towards

all previous members of the group is smaller than a certain threshold ϵ_{S}. In [SK17c], the design parameter ϵ_{S} is evaluated to be optimal in the range of $0.3 \leq \epsilon_{\mathrm{S}} \leq 0.4$, depending on the SINR of the users. Since in this thesis UTs with high G/T, i.e. high SINR values, are considered, the threshold is set to $\epsilon_{\mathrm{S}} = 0.4$.

4 Minimum Secrecy Capacity Precoding

In this chapter, the MSC precoding algorithm is described and evaluated with numerical simulations taking the presented system architecture into account. This includes the problem formulation and the reasoning for the minimum secrecy capacity as a metric of choice, the convex reformulation with an iterative approximation, and the application of AN to improve the secrecy. The numerical analysis validates the effectiveness of the MSC precoding to generate MU-MIMO SATCOM channels suitable for key-less PLS with a certain secrecy capacity.

4.1 Computation of the Precoding Vectors

4.1.1 Problem Formulation

An example of an algorithm to maximize the minimum secrecy capacity is presented in [LLO+19] with the drawback of a total power constraint. The HTS considered in this thesis employs a single HPA per feed and, thus, a PAPC must be taken into account. Since the minimum secrecy capacity is dependent on all user signals in the same way, the set of precoding vectors $(\mathbf{t}_1, \ldots, \mathbf{t}_K)$ must be optimized in a single step. By introducing the system-wide minimum secrecy capacity $C_{S,\min}$ which will be defined in the next section, the final MSC precoding optimization problem is

$$\begin{aligned} \max_{(\mathbf{t}_1,\ldots,\mathbf{t}_K)} \quad & C_{S,\min} \\ \text{subject to} \quad & \left[\sum_{k=1}^{K} \mathbf{t}_k \mathbf{t}_k^{\mathrm{H}}\right]_{l,l} \leq 1, \quad \forall l. \end{aligned} \tag{4.1}$$

4.1.2 Defining the Minimum Secrecy Capacity

The secrecy capacity definition of (2.2) must be extended to solve the MSC precoding problem. The capacity of the kth user is given by [Sha48]

$$C_{\mathrm{B},k} = \log_2(1 + \gamma_{\mathrm{B},k}), \tag{4.2}$$

using the user's SINR $\gamma_{\mathrm{B},k}$ from (3.3). Moreover, the capacity of the mth eavesdropper intercepting and decoding the kth user signal is given by

$$C_{\mathrm{E},mk} = \log_2(1 + \gamma_{\mathrm{E},mk}), \tag{4.3}$$

using the eavesdropper's SINR $\gamma_{\mathrm{E},mk}$ from (3.5). The interference of the other users is treated as noise. The secrecy capacity $C_{S,mk}$ of the kth user towards the mth eavesdropper is defined by the difference of the user capacity $C_{\mathrm{B},k}$ and the mth eavesdropper capacity towards the kth user $C_{\mathrm{E},mk}$:

$$C_{S,mk} = C_{\mathrm{B},k} - C_{\mathrm{E},mk}. \tag{4.4}$$

However, after being able to decode one user signal, an eavesdropper could apply SIC to improve the SINR of other user signals. Hence, the security of the whole system against eavesdropping is limited by the security of the weakest user. Moreover, even the most capable eavesdropper should not be able to intercept any user signal and, therefore, the system-wide minimum secrecy capacity $C_{S,\min}$ is given by

$$C_{S,\min} = \min_{\substack{k=1,\dots,K \\ m=1,\dots,M}} (C_{\mathrm{B},k} - C_{\mathrm{E},mk}). \tag{4.5}$$

4.1.3 Convex Reformulation

In order to solve (4.1) in a computational efficient way, the problem must be reformulated. An auxiliary variable $c_{\min} \in \mathbb{R}$ is introduced. If the secrecy capacities for all users and eavesdroppers are greater or equal $c_{\min}$, then $c_{\min}$ is equal to the minimum secrecy capacity $C_{S,\min}$. Moreover, the user capacity $C_{\mathrm{B},k}$ can be rewritten using (3.3)

$$\begin{aligned} C_{\mathrm{B},k} = \log_2\left(1 + \gamma_{\mathrm{B},k}\right) &= \log_2\left(1 + \frac{\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_k\right|^2}{\sum_{i\neq k}\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_i\right|^2 + \sigma_{w_{\mathrm{B},k}}^2}\right) \\ &= \log_2\left(\frac{\sum_{i=1}^{K}\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_i\right| + \sigma_{w_{\mathrm{B},k}}^2}{\sum_{i\neq k}\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_i\right| + \sigma_{w_{\mathrm{B},k}}^2}\right). \end{aligned} \tag{4.6}$$

Likewise, this can be done for the eavesdropper capacity $C_{\mathrm{E},mk}$ using (3.5). The optimization problem is now

$$\begin{aligned}
\max_{(\mathbf{t}_1,\ldots,\mathbf{t}_K)} \quad & c_{\min} \\
\text{subject to} \quad & c_{\min} \leq (C_{\mathrm{B},k} - C_{\mathrm{E},mk}), && \forall k, \forall m, \\
& C_{\mathrm{B},k} = \log_2\left(\frac{\sum_{i=1}^{K}\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_i\right| + \sigma_{w_{\mathrm{B},k}}^2}{\sum_{i\neq k}\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_i\right| + \sigma_{w_{\mathrm{B},k}}^2}\right), && \forall k, \\
& C_{\mathrm{E},mk} = \log_2\left(\frac{\sum_{i=1}^{K}\left|\mathbf{h}_{\mathrm{E},m}^{\mathrm{H}}\mathbf{t}_i\right| + \sigma_{w_{\mathrm{E},m}}^2}{\sum_{i\neq k}\left|\mathbf{h}_{\mathrm{E},m}^{\mathrm{H}}\mathbf{t}_i\right| + \sigma_{w_{\mathrm{E},m}}^2}\right), && \forall k, \forall m, \\
& \left[\sum_{k=1}^{K}\mathbf{t}_k\mathbf{t}_k^{\mathrm{H}}\right]_{l,l} \leq 1, && \forall l.
\end{aligned} \tag{4.7}$$

The optimization problem must follow the DCP rules [GBY06] like the ZF precoding in Section 3.4.2. Therefore, the matrix $\mathbf{T}_k = \mathbf{t}_k\mathbf{t}_k^{\mathrm{H}} \in \mathbb{C}^{L\times L}$ is introduced and the $\mathrm{rank}(\mathbf{T}_k) = 1$ constraint is skipped:

$$\max_{(\mathbf{T}_1,\ldots,\mathbf{T}_K)} \quad c_{\min} \tag{4.8a}$$

$$\text{subject to} \quad c_{\min} \leq (C_{\mathrm{B},k} - C_{\mathrm{E}mk}), \tag{4.8b}$$

$$C_{\mathrm{B},k} = \log_2\left(\frac{\sum_{i=1}^{K}\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{T}_i\mathbf{h}_{\mathrm{B},k} + \sigma_{w_{\mathrm{B},k}}^2}{\sum_{i\neq k}\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{T}_i\mathbf{h}_{\mathrm{B},k} + \sigma_{w_{\mathrm{B},k}}^2}\right), \quad \forall k, \tag{4.8c}$$

$$C_{\mathrm{E},mk} = \log_2\left(\frac{\sum_{i=1}^{K}\mathbf{h}_{\mathrm{E},m}^{\mathrm{H}}\mathbf{T}_i\mathbf{h}_{\mathrm{E},m} + \sigma_{w_{\mathrm{E},m}}^2}{\sum_{i\neq k}\mathbf{h}_{\mathrm{E},m}^{\mathrm{H}}\mathbf{T}_i\mathbf{h}_{\mathrm{E},m} + \sigma_{w_{\mathrm{E},m}}^2}\right), \quad \forall k, \forall m, \tag{4.8d}$$

$$\left[\sum_{k=1}^{K}\mathbf{T}_k\right]_{l,l} \leq 1, \quad \forall l, \tag{4.8e}$$

$$\mathbf{T}_k \succeq 0, \quad \forall k. \tag{4.8f}$$

For the next steps, let us define the numerator and denominator of (4.6) as the following real-valued auxiliary variables for all $k = 1,\ldots,K$ users and $m = 1,\ldots,M$ eavesdroppers,

respectively:

$$\begin{aligned} s_k &= \ln\left(\sum_{i=1}^{K} \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{T}_i \mathbf{h}_{\mathrm{B},k} + \sigma_{w_{\mathrm{B},k}}^2\right), \\ n_k &= \ln\left(\sum_{i\neq k} \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{T}_i \mathbf{h}_{\mathrm{B},k} + \sigma_{w_{\mathrm{B},k}}^2\right), \\ s_m &= \ln\left(\sum_{i=1}^{K} \mathbf{h}_{\mathrm{E},m}^{\mathrm{H}} \mathbf{T}_i \mathbf{h}_{\mathrm{E},m} + \sigma_{w_{\mathrm{E},m}}^2\right), \\ n_{mk} &= \ln\left(\sum_{i\neq k} \mathbf{h}_{\mathrm{E},m}^{\mathrm{H}} \mathbf{T}_i \mathbf{h}_{\mathrm{E},m} + \sigma_{w_{\mathrm{E},m}}^2\right). \end{aligned} \tag{4.9}$$

Moreover, replacing the capacity constraint (4.8b) by the auxiliary variables in (4.9) leads to:

$$\begin{aligned} c_{\min} &\leq \log_2\left(\frac{\mathrm{e}^{s_k}}{\mathrm{e}^{n_k}}\right) - \log_2\left(\frac{\mathrm{e}^{s_m}}{\mathrm{e}^{n_{mk}}}\right), \\ &= \log_2(\mathrm{e}^{s_k} - \mathrm{e}^{n_k} - \mathrm{e}^{s_m} + \mathrm{e}^{n_{mk}}), \\ &= (s_k - n_k - s_m + n_{mk}) \log_2(\mathrm{e}), \quad \forall k, \forall m. \end{aligned} \tag{4.10}$$

Due to the logarithm, the terms s_k and n_{mk} are concave, whereas the negative terms $-n_k$ and $-s_m$ in (4.10) are convex [BV04]. Hence, as a sum of all these terms, the minimum secrecy capacity auxiliary variable $c_{\min}$ is neither convex nor concave and, thus, violates the DCP rules. The maximization problem in (4.8), however, needs a concave objective function [BV04]. The convex-concave procedure (CCP) is a powerful heuristic method to find local solutions to the so-called difference of convex programming problems [LB16]. In a maximization problem, all convex terms are approximated by a linear lower bound at an initial feasible point. The resulting local optimal solution may depend on the selected initial point and it can be helpful to initialize the algorithm with different starting points and choose the final solution with the highest objective value [LB16].

Approximated lower bounds of n_k and s_m are necessary for the CCP. If $\mathbf{T}_k^{(0)}$ are feasible solutions for the problem (4.8), approximations for n_k and s_m are

$$\begin{aligned} \tilde{n}_k &= \ln\left(\sum_{i\neq k} \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{T}_i^{(0)} \mathbf{h}_{\mathrm{B},k} + \sigma_{w_{\mathrm{B},k}}^2\right), \\ \tilde{s}_m &= \ln\left(\sum_{i=1}^{K} \mathbf{h}_{\mathrm{E},m}^{\mathrm{H}} \mathbf{T}_i^{(0)} \mathbf{h}_{\mathrm{E},m} + \sigma_{w_{\mathrm{E},m}}^2\right). \end{aligned} \tag{4.11}$$

Moreover, the first-order Taylor approximations of e^{n_k} and e^{s_m} at a feasible point $\mathbf{T}_k^{(0)}$ are

$$\begin{aligned} \mathrm{e}^{n_k} &= \mathrm{e}^{\tilde{n}_k} + \mathrm{e}^{\tilde{n}_k}(n_k - \tilde{n}_k), \\ \mathrm{e}^{s_m} &= \mathrm{e}^{\tilde{s}_m} + \mathrm{e}^{\tilde{s}_m}(s_m - \tilde{s}_m). \end{aligned} \tag{4.12}$$

Applying the auxiliary variables (4.9) and (4.10) as well as the first-order Taylor approximations (4.12) to the problem (4.8), the computational efficiently solvable problem is given by:

$$\max_{\substack{s_k, n_k, s_m, n_{mk} \\ (\mathbf{T}_1, \ldots, \mathbf{T}_K)}} \quad c_{\min} \tag{4.13a}$$

$$\text{subject to} \quad c_{\min} \leq (s_k - n_k - s_m + n_{mk}) \log_2(\mathrm{e}), \tag{4.13b}$$

$$\sum_{i=1}^{K} \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{T}_i \mathbf{h}_{\mathrm{B},k} + \sigma_{w_{\mathrm{B},k}}^2 \geq \mathrm{e}^{s_k}, \qquad \forall k, \tag{4.13c}$$

$$\sum_{i \neq k} \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{T}_i \mathbf{h}_{\mathrm{B},k} + \sigma_{w_{\mathrm{B},k}}^2 = \mathrm{e}^{\tilde{n}_k}(n_k - \tilde{n}_k + 1), \qquad \forall k, \tag{4.13d}$$

$$\sum_{i=1}^{K} \mathbf{h}_{\mathrm{E},m}^{\mathrm{H}} \mathbf{T}_i \mathbf{h}_{\mathrm{E},m} + \sigma_{w_{\mathrm{E},m}}^2 = \mathrm{e}^{\tilde{s}_m}(s_m - \tilde{s}_m + 1), \quad \forall m, \tag{4.13e}$$

$$\sum_{i \neq k} \mathbf{h}_{\mathrm{E},m}^{\mathrm{H}} \mathbf{T}_i \mathbf{h}_{\mathrm{E},m} + \sigma_{w_{\mathrm{E},m}}^2 \geq \mathrm{e}^{n_{mk}}, \qquad \forall k, \forall m, \tag{4.13f}$$

$$\left[\sum_{k=1}^{K} \mathbf{T}_k \right]_{l,l} \leq 1, \qquad \forall l, \tag{4.13g}$$

$$\mathbf{T}_k \succeq 0, \qquad \forall k. \tag{4.13h}$$

The inequalities (4.13c) and (4.13f) are necessary due to the DCP rules and hold with equality for the final solution. If e^{s_k} and $\mathrm{e}^{n_{mk}}$ could be further increased, the value of the objective $c_{\min}$ would be increased as well.

Solving (4.13) at an initial feasible point $\mathbf{T}_k^{(0)}$, the resulting optimal $\mathbf{T}_k^{\circledast(1)}$ can be used as the starting point of the next iteration. The auxiliary variables are updated by:

$$\begin{aligned} \tilde{n}_k^{(j)} &= \ln\left(\sum_{i \neq k} \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{T}_i^{\circledast(j)} \mathbf{h}_{\mathrm{B},k} + \sigma_{w_{\mathrm{B},k}}^2 \right), \\ \tilde{s}_m^{(j)} &= \ln\left(\sum_{i=1}^{K} \mathbf{h}_{\mathrm{E},m}^{\mathrm{H}} \mathbf{T}_i^{\circledast(j)} \mathbf{h}_{\mathrm{E},m} + \sigma_{w_{\mathrm{E},m}}^2 \right). \end{aligned} \tag{4.14}$$

The iterative process stops when a maximum number of iterations $J_{\max}$ is reached or

when the objective value $c_{\min}$ has not been improved by a value higher than a threshold ϵ_{O}, i.e. $c_{\min}^{(j)} - c_{\min}^{(j-1)} < \epsilon_{\mathrm{O}}$. In case of a similar objective value, a local optimum has been found. The initial objective value is set to $c_{\min}^{(0)} = -\infty$ (or any large negative number) to enforce at least a second iteration. The CCP algorithm to find a locally optimal solution for the MSC precoding problem (4.1) is shown in Fig. 4.1. The convergence of the CCP is proofed in [LB16]. However, the locally optimal solution may be dependent on the initial feasible point. Different initial feasible points are evaluated in Section 4.2.1. The SDR matrices $\mathbf{T}_k^{\circledast}$ must be turned back into precoding vectors (cf. Section 3.4.2). If there are any matrices with $\operatorname{rank}\left(\mathbf{T}_k^{\circledast}\right) > 1$, the suboptimal result of the Gaussian randomization process from Fig. 3.5 may lead to a smaller minimum secrecy capacity than the final objective value $c_{\min}^{(j)}$.

Data: Initial feasible precoding matrices $\mathbf{T}_k^{(0)}$
Maximum number of iterations $J_{\max}$
Threshold ϵ_{O}
Result: Locally optimal precoding vectors $\mathbf{t}_k^{\circledast}$
$j = 0$
repeat
Compute auxiliary variables $\tilde{n}_k^{(j)}$ and $\tilde{s}_m^{(j)}$ using (4.14)
Set $\mathbf{T}_k^{\circledast(j+1)}$ to the solution of the optimization problem (4.13)
Update iteration $j = j + 1$
until $c_{\min}^{(j)} - c_{\min}^{(j-1)} < \epsilon_{\mathrm{O}}$ *or* $j \geq J_{\max}$
Compute $\mathbf{t}_k^{\circledast}$ with eigendecomposition or Gaussian randomization

Figure 4.1: Convex-concave procedure algorithm to find a locally optimal solution for the MSC precoding.

4.1.4 Adding Artificial Noise

The application of AN may improve the minimum secrecy capacity or even be necessary to achieve secrecy at all [GN08]. The derivation of the optimization problem is similar to the precoding without AN. The capacities in (4.2) and (4.3) are redefined with the SINR values of the users $\gamma_{\mathrm{B},k}^{\mathrm{AN}}$ from (3.7) and the SINR values of the eavesdroppers $\gamma_{\mathrm{E},mk}^{\mathrm{AN}}$ from (3.8) instead. Additionally, the matrix $\mathbf{T}_a = \mathbf{t}_a \mathbf{t}_a^{\mathrm{H}} \in \mathbb{C}^{L \times L}$ is defined which has to be positive semidefinite and the rank-one constraint is dropped to convexify the problem.

This leads to the problem formulation

$$
\begin{aligned}
\max_{\substack{s_k,n_k,s_m,n_{mk}\\(\mathbf{T}_1,\ldots,\mathbf{T}_K,\mathbf{T}_a)}} \quad & c_{\min} \\
\text{subject to} \quad & c_{\min} \leq (s_k - n_k - s_m + n_{mk}) \log_2(\mathrm{e}), \\
& \sum_{i=1}^{K} \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{T}_i \mathbf{h}_{\mathrm{B},k} + \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{T}_a \mathbf{h}_{\mathrm{B},k} + \sigma_{w_{\mathrm{B},k}}^2 \geq \mathrm{e}^{s_k}, && \forall k, \\
& \sum_{i\neq k} \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{T}_i \mathbf{h}_{\mathrm{B},k} + \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{T}_a \mathbf{h}_{\mathrm{B},k} + \sigma_{w_{\mathrm{B},k}}^2 = \mathrm{e}^{\tilde{n}_k}(n_k - \tilde{n}_k + 1), && \forall k, \\
& \sum_{i=1}^{K} \mathbf{h}_{\mathrm{E},m}^{\mathrm{H}} \mathbf{T}_i \mathbf{h}_{\mathrm{E},m} + \mathbf{h}_{\mathrm{E},m}^{\mathrm{H}} \mathbf{T}_a \mathbf{h}_{\mathrm{E},m} + \sigma_{w_{\mathrm{E},m}}^2 = \mathrm{e}^{\tilde{s}_m}(s_m - \tilde{s}_m + 1), && \forall m, \\
& \sum_{i\neq k} \mathbf{h}_{\mathrm{E},m}^{\mathrm{H}} \mathbf{T}_i \mathbf{h}_{\mathrm{E},m} + \mathbf{h}_{\mathrm{E},m}^{\mathrm{H}} \mathbf{T}_a \mathbf{h}_{\mathrm{E},m} + \sigma_{w_{\mathrm{E},m}}^2 \geq \mathrm{e}^{n_{mk}}, && \forall k, \forall m, \\
& \left[\sum_{k=1}^{K} \mathbf{T}_k + \mathbf{T}_a\right]_{l,l} \leq 1, && \forall l, \\
& \mathbf{T}_a \succeq 0, \mathbf{T}_k \succeq 0, && \forall k.
\end{aligned}
\tag{4.15}
$$

Null space AN beamforming is not considered. The additional constraints such that $\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{t}_a\right|^2 = 0$ further restrict the optimization problem without any benefit. The AN is already included in the user SINR terms. Furthermore, since the computational complexity of an SDP in (3.22) also depends on the number of constraints, this would decrease the execution speed. The optimization problem with artificial noise can be solved with the algorithm shown in Fig. 4.2. A secure transmission is now possible with the resulting precoding vectors.

4.2 Numerical Analysis

In this section, numerical simulations, i.e. Monte-Carlo simulations, are performed to evaluate the MSC precoding algorithm. Taking the scenario from Section 3.1.2 into account, different initialization strategies for the CCP, the secrecy performance with multiple eavesdroppers and the secrecy region are investigated.

4.2.1 Initialization Strategies for the Convex-Concave Procedure

As stated in [LB16], the the final, locally optimal, solutions of the precoding vectors $\mathbf{t}_k^{\circledast}$ are influenced by the initial feasible solutions $\mathbf{T}_k^{(0)} = \mathbf{t}_k^{(0)} \mathbf{t}_k^{(0)^{\mathrm{H}}}$ provided to the CCP

Data: Initial feasible precoding matrices $\mathbf{T}_k^{(0)}$ and $\mathbf{T}_a^{(0)}$
Maximum number of iterations $J_{\max}$
Threshold ϵ_{O}
Result: Locally optimal precoding vectors $\mathbf{t}_k^{\circledast}$ and $\mathbf{t}_a^{\circledast}$
$j = 0$
repeat
Compute auxiliary variables $\tilde{n}_k^{(j)}$ and $\tilde{s}_m^{(j)}$ using (4.14)
Set $\mathbf{T}_k^{\circledast(j+1)}$ and $\mathbf{T}_a^{\circledast(j+1)}$ to the solution of the optimization problem (4.15)
Update iteration $j = j + 1$
until $c_{\min}^{(j)} - c_{\min}^{(j-1)} < \epsilon_{\mathrm{O}}$ *or* $j \geq J_{\max}$
Compute $\mathbf{t}_k^{\circledast}$ and $\mathbf{t}_a^{\circledast}$ with eigendecomposition or Gaussian randomization

Figure 4.2: Convex-concave procedure algorithm to find a locally optimal solution for the MSC precoding with AN.

algorithm in Fig. 4.1. Therefore, three different strategies are evaluated:

1. ***ZF Precoding***: The vectors $\mathbf{t}_k^{(0)}$ are initialized with the solutions of the ZF precoding with the fairness objective given in (3.19).

2. ***Beam Gain***: The kth user signal is fully transmitted in that beam l_k^* where the amplitude of the channel propagation coefficient is the highest. If that beam is already occupied by another user, the second highest is chosen. The initial feasible solution for user k is a vector of zeros with a 1 at the index l_k^*.

3. ***Random***: The vectors $\mathbf{t}_k^{(0)}$ are set to random vectors $\boldsymbol{\xi}_k \sim \mathcal{CN}(0, \mathbf{I}_L)$ which are scaled such that $|\boldsymbol{\xi}_k|^2 = 1/K$, i.e. each user signal is transmitted in each beam with power $1/K$.

The relevant parameters of the CCP in Algorithm 4.1 are the number of iterations, the final minimum secrecy capacity $c_{\min}$ and the probability of rank-one solutions of $\mathbf{T}_k^{\circledast}$ and $\mathbf{T}_a^{\circledast}$ to avoid the suboptimal Gaussian randomization process. Table 4.1 summarizes the relevant parameters of the MSC precoding algorithm for the different initialization strategies. In the performed Monte-Carlo simulations, the following parameters were set additionally: maximum number of iterations $J_{\max} = 10$ and threshold $\epsilon_{\mathrm{O}} = 0.001\,\mathrm{b/s/Hz}$. Strategies with a smaller average number of iterations have an improved runtime performance and may be favored. Since the ZF precoding is already an optimization problem which must be solved, the number of iterations in Algorithm 4.1 for the *ZF precoding* strategy should be increased by 1 for a fair comparison with the other two strategies. Fig. 4.3 shows the distribution of the minimum secrecy capacities in dependency of the

initialization strategies. The best-case and worst-case performances of all strategies are approximately equal. However, the initialization with *ZF precoding* performs 0.1 b/s/Hz better on average. The overperformance gives an indication in how many Monte-Carlo runs the strategy performs at least 5 % better than the others in terms of $c_{\min}$. Moreover, the percentages of rank-one solutions $\mathbf{T}_k^{\circledast}$ is given in the last columns. The Gaussian randomization procedure is suboptimal and more computationally expensive than the eigendecomposition and, hence, many rank-one matrices are beneficial.

In conclusion, the *ZF precoding* initialization strategy takes the least number of iterations and leads to the best performance with an approximately equal percentage of rank-one solutions. Hence, it is the initialization strategy of choice and will be used in all MSC precoding algorithm computations throughout this thesis. The rare cases when *Beam Gain* or *Random* perform better can be neglected.

Table 4.1: Comparison of the Initialization Strategies for the CCP

Strategy	**Avg. Number of Iterations**		**Overperformance**		**Rank-one Solutions**	
		with AN		with AN		with AN
ZF Prec.	5.34 (+1)	3.57 (+1)	1 %	9 %	94 %	95 %
Beam Gain	7.28	4.65	1 %	1 %	94 %	97 %
Random	7.52	5.44	0 %	1 %	94 %	96 %

4.2.2 Secrecy Capacity Performance

The secrecy capacity performance of the MSC precoding without and with AN, respectively, is investigated in the case of different numbers of eavesdroppers. In particular, the case where the number of eavesdroppers exceeds the number of beams is analyzed. Therefore, the exemplary scenario from Section 3.1.2 is simulated. Moreover, a comparison between the MR antenna design and a single reflector is provided. In general, absolute capacity values are only due to the chosen scenario and are not directly comparable. Because of this, the ZF precoding user capacity is given as an approximate upper bound of the minimum secrecy capacity which could be achieved only when no eavesdropper is present.

4.2.2.1 MSC Precoding without and with AN

In Fig. 4.4, the minimum secrecy capacity distribution for $M = 2$ and $M = 8$ eavesdroppers is shown for MSC precoding without and with AN. Moreover, Table 4.2 summarizes the

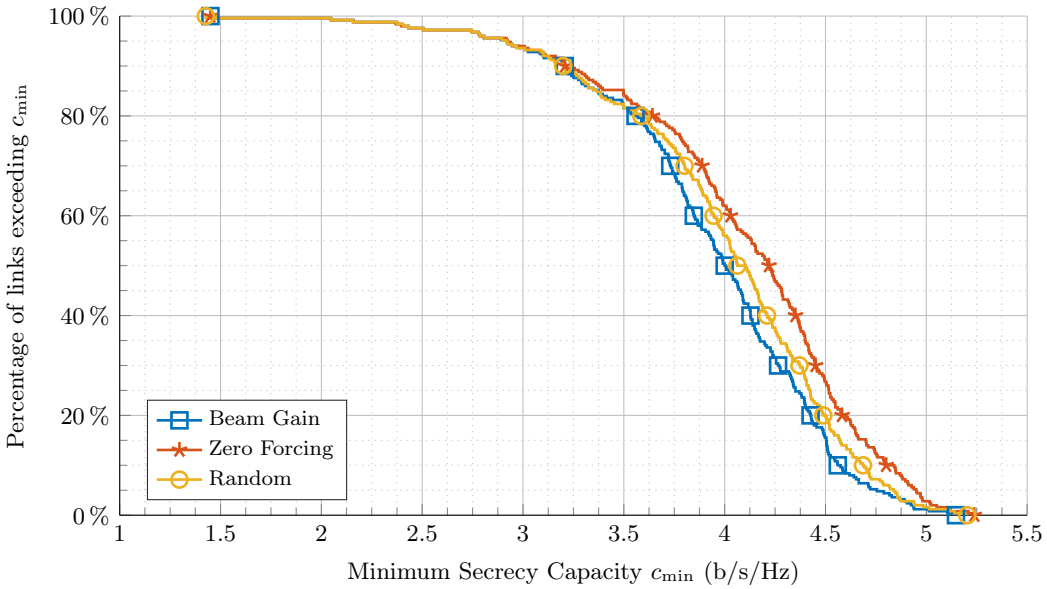

Figure 4.3: Minimum secrecy capacity distribution for different initialization strategies

average minimum secrecy capacity $\mathrm{E}[c_{\min}]$ and the power usage for $M = 2$, $M = 4$, and $M = 8$. In case of $M = 2$, the increase of minimum secrecy capacity by use of AN is minimal. In general, when the MIMO degrees of freedom are sufficient, i.e. $L \geq K + M$, AN does not provide a significant secrecy advantage. However, with more eavesdropper, the impact of AN is obvious with an increase from 2.85 b/s/Hz to 3.27 b/s/Hz on average. The utilization of AN is useful in cases where $L < K + M$. Since a larger part of the available power must be spent for the AN, the achievable minimum secrecy capacity is decreased compared to the $M = 2$ case. However, the worst case with $M = 8$ resulting in $c_{\min} = 0.45$ b/s/Hz is only due to the fact that one user and the 7th eavesdropper are only 4 km apart. The precoding with users and eavesdroppers close to each other is difficult because of the similar CSI in LOS SATCOM. This can happen with fewer eavesdroppers as well, but the chance that a user is close to an eavesdropper is higher with more eavesdroppers.

To summarize the results, secrecy can always be achieved by means of AN but does not provide significant secrecy gains in cases of $L \geq K + M$. Eavesdropper positions close to users are most critical. However, that circumstance cannot be avoided either by the system operator or the design of the precoding algorithm since it depends on the underlying problem of similar channels. Technically, a higher distance of the antennas in space, e.g. . with collocated satellites [Sch19], allow for smaller user / eavesdropper spacings on Earth with an increased difficulty on CSI estimation.

Table 4.2: Secrecy Capacity Performance and Power Usage with Multiple Eavesdroppers

Eves	**MSC**	**MSC with AN**		**ZF**
	Avg. Minimum Secrecy Capacity E[$c_{\min}$]			Avg. User Capacity E[C_{B}]
				5.40 b/s/Hz
$M = 2$	4.00 b/s/Hz	4.09 b/s/Hz		
$M = 4$	3.68 b/s/Hz	3.81 b/s/Hz		
$M = 8$	2.85 b/s/Hz	3.27 b/s/Hz		
	Average Power Usage (% of total available power)			
	User	User	AN	User
				100%
$M = 2$	99.9%	85.4%	11.5%	
$M = 4$	99.4%	84.4%	14.3%	
$M = 8$	99.4%	76.5%	20.9%	

4.2.2.2 Comparison of MR Antenna Design and a Single Reflector

Fig. 4.5 includes a comparison of the minimum secrecy capacity distribution and ZF user capacity applying the proposed MR antenna design or a single reflector on the satellite. Even though the gain of AN is not high for $M = 2$, the MSC with AN performs better for both antenna schemes. Keep in mind that due to the complementary cumulative distribution function shown in Fig. 4.5, the worst case ZF user capacity is not directly related to the worst case minimum secrecy capacity. In direct proportion, the MR antenna design achieves a minimum secrecy capacity of 75.7 % of the ZF user capacity on average with a range of 27.2 % to 90.1 %. By contrast, the average fraction applying the SR scheme is only 41.8 % with a range of 0 % to 121.2 %. In other words, in the worst case no secrecy can be achieved at all, whereas in the best case, the minimum secrecy capacity of the MSC precoding with AN is higher than the respective ZF precoding for this user group. In conclusion, the MR antenna design shows superior secrecy capacity performance compared to the SR antenna design on a percentage basis as well as on absolute values. The minimum secrecy capacity with MR antennas is often even higher than the ZF user capacity with a SR antenna.

4.2.3 Secrecy Region

The secrecy region gives insight into the areas where the secrecy capacity C_S is above a certain threshold, e.g. 2.00 b/s/Hz, to guarantee secure data transmission for the users.

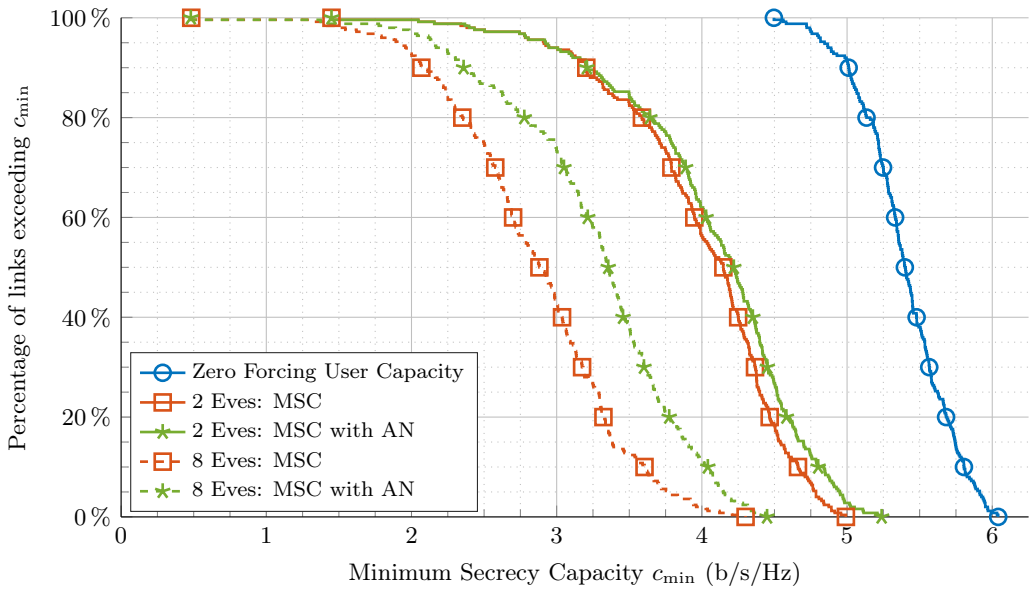

Figure 4.4: Minimum secrecy capacity distribution and ZF user capacity for multiple user groups in case of $M = 2$ and $M = 8$ eavesdroppers

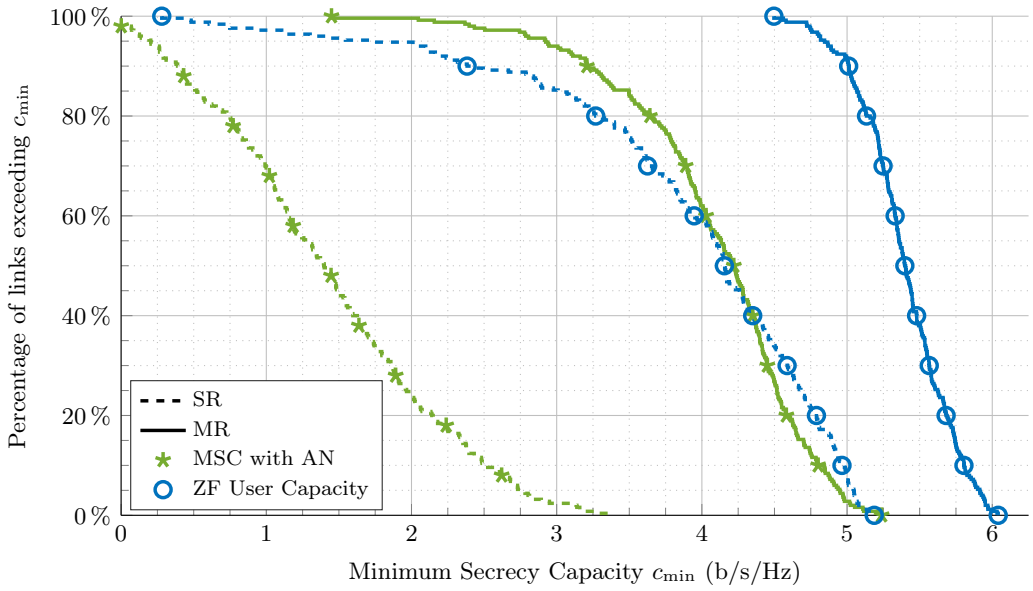

Figure 4.5: Minimum secrecy capacity distribution and ZF user capacity for multiple user groups for SR and MR antenna design in case of $M = 2$ eavesdroppers

Conversely, the vulnerability region is the aggregation of areas where an eavesdropper unknown to the system provider potentially can intercept user signals. Referring to Fig. 4.4, a minimum secrecy capacity above 2.00 b/s/Hz is achieved in 97 % of the user groups applying the MSC precoding with AN in case of $M = 8$ eavesdroppers. Furthermore, a secure channel code achieving the secrecy capacity of 2.00 b/s/Hz is considered to exist. The areas in which the secrecy capacity cannot achieve the target value, i.e. $C_S \leq 2.00$ b/s/Hz, are exemplarily illustrated by blue and orange contour lines in Fig. 4.6. Receivers in these areas can potentially decode the secure messages. This is why the users are always located inside these areas. The VR plots are drawn assuming the same powerful eavesdroppers like in the other simulations at any location. The areas are randomly distributed and proportionally small compared to the diameter of the beams in the given scenario. The two user positions are marked with B_1 and B_2 and eight eavesdropper positions with E_1 to E_8, respectively. Please note that the contour lines are the result of the users' and eavesdroppers' locations of this particular example. They will be different if the locations change. Inside the blue and orange contour lines, at least one of the user data streams is interceptable with a secrecy capacity below 2.00 b/s/Hz, whereas the blue contour lines indicate the VR of user B_1 and the orange ones the VR of user B_2, respectively. The users are inside of the contour areas of course so that they are able to receive the data intended for them. However, all eight eavesdroppers are located outside of the contour areas, i.e. secure communication to user B_1 and B_2 is achieved. Even if potential eavesdroppers install huge dish antennas to achieve an enormous receiver G/T of 37.5 dB/K instead of the typically assumed 25.5 dB/K, the VR only slightly increases which is shown in comparison of Fig. 4.6 (a) and (b).

Since the minimum secrecy capacity performance of the SR scenario, i.e. $L_R = 1$, is lower in general, the target secrecy capacity is reduced to 0.50 b/s/Hz and the areas in which the secrecy capacity is below this target value, i.e. $C_S \leq 0.50$ b/s/Hz, are exemplarily illustrated by blue and orange contour lines in Fig. 4.6. The VR for each user data stream is large and contiguous. This result has also been presented in [SKS19]. Moreover, with an increased G/T of the eavesdroppers, this area increases noticeable. For potential new eavesdroppers unknown to the system operator, it the therefore comparatively easy to find a location for interception of the user signals.

4.2.4 Concept of Virtual Eavesdroppers

Considering the possibility that the secure data can be split into multiple consecutive blocks such that it is necessary to receive and decode all blocks to recover the data, the concept of virtual eavesdroppers is helpful to further reduce the VR. Since the MSC

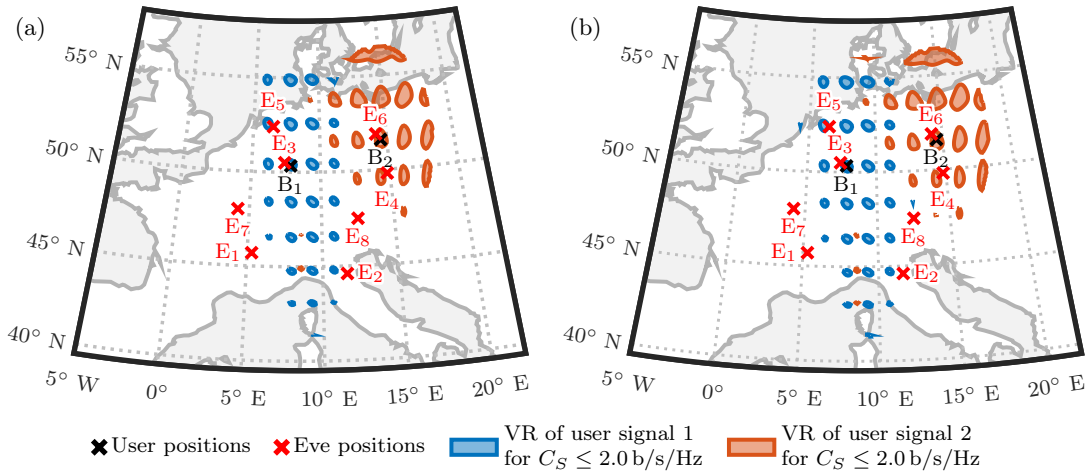

Figure 4.6: Vulnerability regions of the secrecy capacity with $M = 8$ eavesdroppers comprising a receiver with (a) +6 dB/K and (b) +18 dB/K relative to the default UTs in an MR antenna design

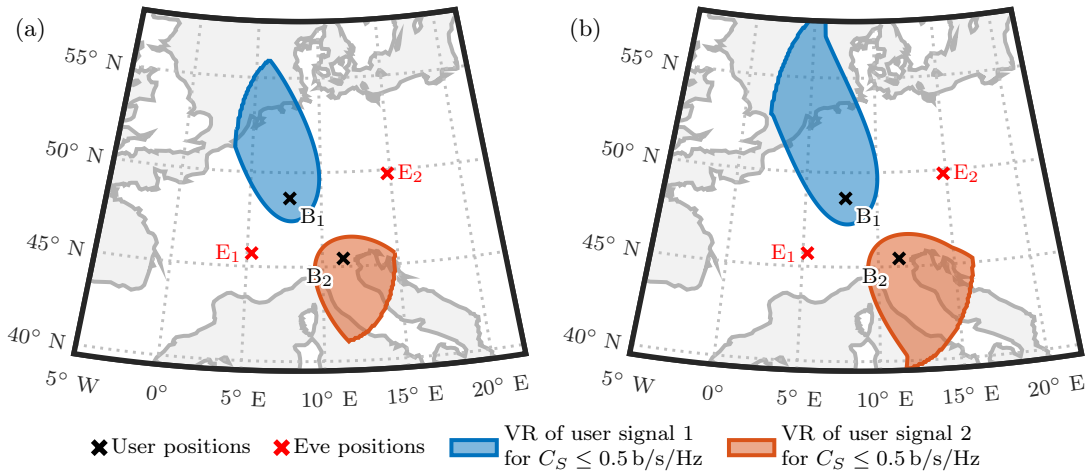

Figure 4.7: Vulnerability regions of the secrecy capacity with $M = 2$ eavesdroppers comprising a receiver with (a) +6 dB/K and (b) +18 dB/K relative to the default UTs in an SR antenna design

optimization is a CCP with locally optimal solutions, the result of the procedure is also strongly influenced by the eavesdropper CSI used for the optimization. Hence, it is proposed to introduce virtual eavesdroppers, i.e. eavesdroppers which do not exist in real with a solely purpose of enforcing varying precoding vectors. For that, random locations are chosen which are many kilometers away from real eavesdroppers and the scheduled users. Locations close to the users would harm the secrecy performance and the benefit of virtual eavesdroppers close to real ones is minimal. The virtual eavesdroppers' CSI is estimated just like for the real ones in Section 3.3.2. Eventually, the MSC precoding algorithm does not distinguish between real and virtual eavesdroppers. The beamforming for each block is performed with the MSC precoding vectors resulting from the optimization with different virtual eavesdroppers additionally to the real ones.

As an example, four sets of MSC precoding vectors with AN are computed considering two users B_1 and B_1, two real eavesdroppers E_1 and E_2, and in each step one virtual eavesdropper E_V. It is shown in Fig. 4.8 that a varying position of the virtual eavesdropper E_V leads to altered areas where the secrecy capacity $C_S \leq 2.00\,\mathrm{b/s/Hz}$. The minimum secrecy capacity as the objective of the optimization is in (a) $c_{\min} = 4.91\,\mathrm{b/s/Hz}$, (b) $c_{\min} = 5.00\,\mathrm{b/s/Hz}$, (c) $c_{\min} = 4.72\,\mathrm{b/s/Hz}$, and (d) $c_{\min} = 4.70\,\mathrm{b/s/Hz}$. The VR areas without a virtual eavesdropper are similar to Fig. 4.8a and, hence, not shown separately. Moreover, the comparison of (b), (c), and (d) of Fig. 4.8 demonstrate that a small VR is not necessarily related to a low $c_{\min}$ and vice versa. To eavesdrop the complete user data, in all of the four blocks a secrecy capacity below $2.00\,\mathrm{b/s/Hz}$ is necessary. Hence, the areas where this requirement is met are drawn in Fig. 4.9 to show the gain of the concept of virtual eavesdroppers.

4.3 Summary

The optimization problem of maximizing the minimum secrecy capacity for multiple users and multiple eavesdroppers under a PAPC is formulated. For a typical HTS scenario with a single amplifier per illuminated beam and users with equal throughput requirements, this precoding algorithm solves the drawbacks of existing literature. The nonconvex problem is reformulated with help of the SDR and the CCP such that the optimization problem follows the DCP rules. Efficient off-the-shelf numerical optimization methods can be used to solve the problem in polynomial time. The CCP algorithm finds a locally optimal solution for the MSC precoding problem after some iterations. AN is added to assist in generating interference at the eavesdroppers to achieve secure communications.

The numerical simulations emphasize the effectiveness of the MSC precoding algorithm

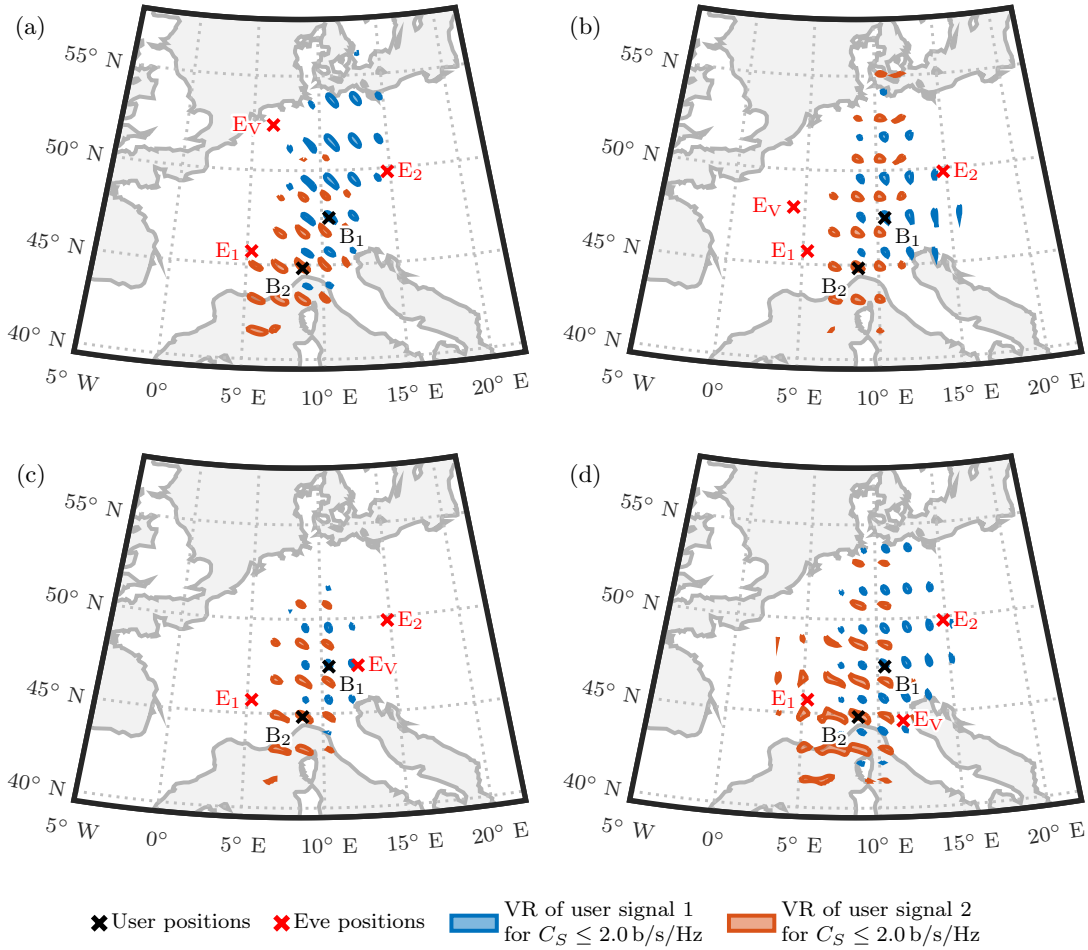

Figure 4.8: Vulnerability regions of the secrecy capacity with $M = 2$ real eavesdroppers and a random virtual eavesdropper for consecutive precoding computations

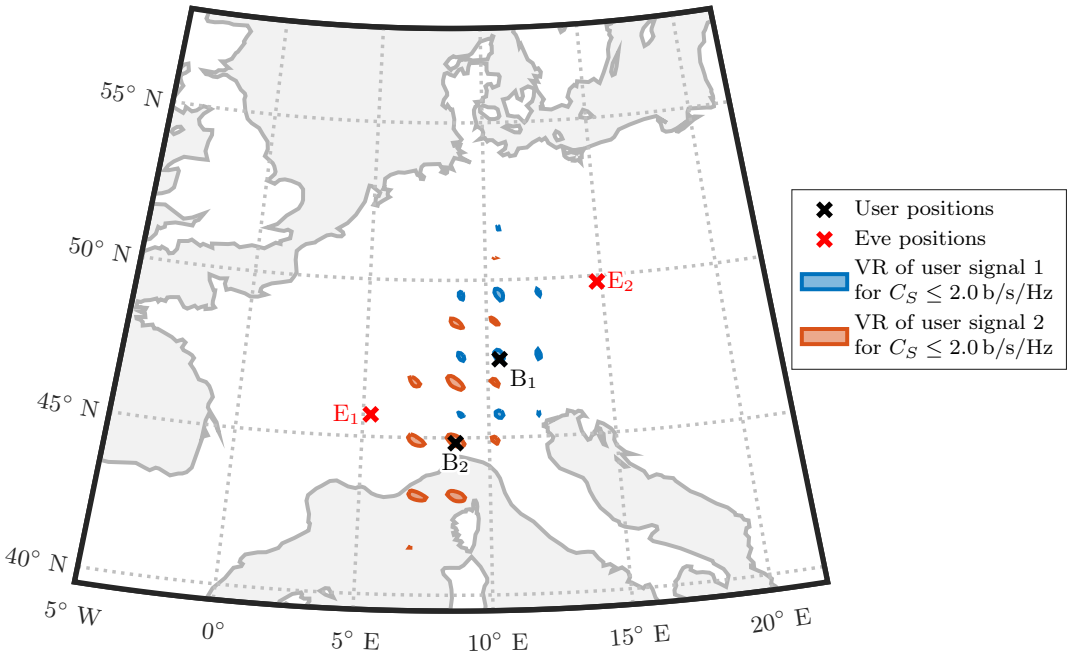

Figure 4.9: Vulnerability regions where in all of the four precoding computations of Fig. 4.8 the secrecy capacity is below the threshold

in the considered HTS scenario. Due to the assumption of powerful eavesdroppers located in the center of the beams, state-of-the-art SISO links can be overheard for sure. As an initial feasible solution is necessary for the CCP, multiple strategies are proposed and evaluated based on the average number of iterations and their secrecy performance. For key-less PLS, the MR antenna design provides huge secrecy gains compared to the SR antenna. The ZF user capacity as an upper bound helps to compare the secrecy capacity performance. The spatial degree of freedom provided by a satellite system with multiple reflector antennas can be exploited to increase the minimum secrecy capacity and decrease the VRs. Moreover, by additionally considering AN signals, the MSC algorithm can cover the case where the number of eavesdroppers exceeds the number of available beams and still achieve PLS. This makes the algorithm suitable also to scenarios where the unscheduled users can be considered as unauthorized users, i.e. confidentiality is ensured also between different users. At the end, virtual eavesdroppers may be used to alter the resulting precoding vectors from frame to frame and further reduce the VR.

5 Security Gap Precoding

The SG precoding algorithms presented in this chapter include multiple strategies to add AN. Besides that, the convex reformulation and the selection of appropriate ACM schemes is given. The numerical analysis validates the effectiveness of the different SG precodings to generate MU-MIMO SATCOM channels suitable for key-less PLS with a certain security gap.

5.1 Computation of the Precoding Vectors

5.1.1 Problem Formulation

In terrestrial communications, the minimization of the total transmission power under the user SINR constraint is performed [RTL98]. The goal of this optimization is to reduce the interference with other users or systems by minimizing the transmitted signal power while maintaining a minimum quality of service (QoS) requirement for each user. The user SINR given in (3.3) must be larger than a minimum SINR $\gamma_{\mathrm{B},k,\min}$ (reliability threshold) to ensure the QoS requirement of the link. The ACM scheme at the transmitter, i.e. the modulation and channel coding rate, can be chosen according to the minimum SINR. While designing the precoding for SATCOM, the PAPC aspect given in (5.1c) has to be considered. The QoS precoding is given by

$$\min_{(\mathbf{t}_1,\ldots,\mathbf{t}_K)} \quad \mathrm{tr}\left(\sum_{k=1}^{K} \mathbf{t}_k \mathbf{t}_k^{\mathrm{H}}\right) \tag{5.1a}$$

$$\text{subject to} \quad \frac{\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{t}_k\right|^2}{\sum_{i \neq k} \left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{t}_i\right|^2 + \sigma_{w_{\mathrm{B},k}}^2} \geq \gamma_{\mathrm{B},k,\min}, \quad \forall k, \tag{5.1b}$$

$$\left[\sum_{k=1}^{K} \mathbf{t}_k \mathbf{t}_k^{\mathrm{H}}\right]_{l,l} \leq 1, \qquad \forall l. \tag{5.1c}$$

To enable the algorithm for PLS with security gap metric, the constraint (5.2d) is added to limit the SINR at the eavesdroppers to the maximum $\gamma_{\mathrm{E},mk,\max}$ (security threshold).

This ensures a security gap of at least $\gamma_{\mathrm{G},mk} = \gamma_{\mathrm{B},k,\min}/\gamma_{\mathrm{E},mk,\max}$. Thus, individual security gap constraints can be defined to serve users with various security demands simultaneously. For users without need of secure communications, the constraint (5.2d) is dropped for this user.

$$\begin{aligned}
\min_{(\mathbf{t}_1,\ldots,\mathbf{t}_K)} \quad & \operatorname{tr}\left(\sum_{k=1}^{K} \mathbf{t}_k \mathbf{t}_k^{\mathrm{H}}\right) && && \text{(5.2a)}\\
\text{subject to} \quad & \frac{\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{t}_k\right|^2}{\sum_{i\neq k}\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{t}_i\right|^2 + \sigma_{w_{\mathrm{B},k}}^2} \geq \gamma_{\mathrm{B},k,\min}, && \forall k, && \text{(5.2b)}\\
& \left[\sum_{k=1}^{K} \mathbf{t}_k \mathbf{t}_k^{\mathrm{H}}\right]_{l,l} \leq 1, && \forall l, && \text{(5.2c)}\\
& \frac{\left|\mathbf{h}_{\mathrm{E},m}^{\mathrm{H}} \mathbf{t}_k\right|^2}{\sum_{i\neq k}\left|\mathbf{h}_{\mathrm{E},m}^{\mathrm{H}} \mathbf{t}_i\right|^2 + \sigma_{w_{\mathrm{E},m}}^2} \leq \gamma_{\mathrm{E},mk,\max}, && \forall k, \forall m. && \text{(5.2d)}
\end{aligned}$$

5.1.2 Convex Reformulation

The optimization problem (5.2) is nonconvex and cannot be solved efficiently in this form. A reformulation to an SDP problem like in Section 3.4.2 is performed to convexify it. First, the positive semidefinite $\mathbf{T}_k = \mathbf{t}_k \mathbf{t}_k^{\mathrm{H}} \in \mathbb{C}^{L\times L}$ are introduced and the rank-one constraint is dropped. Moreover, the division in the reliability and security threshold constraints violate the DCP rules. Since the interference plus noise terms, e.g. $\left(\sum_{i\neq k} \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{T}_i \mathbf{h}_{\mathrm{B},k} + \sigma_{w_{\mathrm{B},k}}^2\right)$, are strictly positive, the multiplication does not inverse the inequality. The following problem (5.3) can be solved efficiently with off-the-shelf numerical optimization methods:

$$\begin{aligned}
\min_{(\mathbf{T}_1,\ldots,\mathbf{T}_K)} \quad & \operatorname{tr}\left(\sum_{k=1}^{K} \mathbf{T}_k\right) && &&\\
\text{subject to} \quad & \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{T}_k \mathbf{h}_{\mathrm{B},k} \geq \gamma_{\mathrm{B},k,\min}\left(\sum_{i\neq k} \mathbf{h}_{\mathrm{B},k}^{\mathrm{H}} \mathbf{T}_i \mathbf{h}_{\mathrm{B},k} + \sigma_{w_{\mathrm{B},k}}^2\right), && \forall k, &\\
& \left[\sum_{k=1}^{K} \mathbf{T}_k\right]_{l,l} \leq 1, && \forall l, & \text{(5.3)}\\
& \mathbf{h}_{\mathrm{E},m}^{\mathrm{H}} \mathbf{T}_k \mathbf{h}_{\mathrm{E},m} \leq \gamma_{\mathrm{E},mk,\max}\left(\sum_{i\neq k} \mathbf{h}_{\mathrm{E},m}^{\mathrm{H}} \mathbf{T}_i \mathbf{h}_{\mathrm{E},m} + \sigma_{w_{\mathrm{E},m}}^2\right), && \forall k, \forall m, &\\
& \mathbf{T}_k \succeq 0, && \forall k. &
\end{aligned}$$

5.1.3 Adding Artificial Noise

The application of AN can improve the possibility to achieve the requested security gap or even be necessary to achieve enough interference for the low SINR values of the eavesdroppers at all [GN08]. The derivation of the optimization problem is similar to the SG precoding without AN. Two different strategies to the application of AN are possible.

Considering the SINR values of the users $\gamma_{\mathrm{B},k}^{\mathrm{AN}}$ from (3.7) and the SINR values of the eavesdroppers $\gamma_{\mathrm{E},mk}^{\mathrm{AN}}$ from (3.8) instead and replacing the SINR values in (5.2) is the first strategy. The total transmission power is minimized to result in an energy efficient solution. A similar strategy has been proposed in [LCMC11]. This leads to the SG with AN precoding problem formulation

$$\min_{(\mathbf{t}_1,\ldots,\mathbf{t}_K,\mathbf{t}_a)} \quad \mathrm{tr}\left(\sum_{k=1}^{K}\mathbf{t}_k\mathbf{t}_k^{\mathrm{H}}+\mathbf{t}_a\mathbf{t}_a^{\mathrm{H}}\right) \tag{5.4a}$$

$$\text{subject to} \quad \frac{\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_k\right|^2}{\sum_{i\neq k}\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_i\right|^2+\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_a\right|^2+\sigma_{w_{\mathrm{B},k}}^2}\geq\gamma_{\mathrm{B},k,\min}, \qquad \forall k, \tag{5.4b}$$

$$\left[\sum_{k=1}^{K}\mathbf{t}_k\mathbf{t}_k^{\mathrm{H}}+\mathbf{t}_a\mathbf{t}_a^{\mathrm{H}}\right]_{l,l}\leq 1, \qquad \forall l, \tag{5.4c}$$

$$\frac{\left|\mathbf{h}_{\mathrm{E},m}^{\mathrm{H}}\mathbf{t}_k\right|^2}{\sum_{i\neq k}\left|\mathbf{h}_{\mathrm{E},m}^{\mathrm{H}}\mathbf{t}_i\right|^2+\left|\mathbf{h}_{\mathrm{E},m}^{\mathrm{H}}\mathbf{t}_a\right|^2+\sigma_{w_{\mathrm{E},m}}^2}\leq\gamma_{\mathrm{E},mk,\max}, \quad \forall k,\forall m. \tag{5.4d}$$

The second strategy called SG with Full Power AN precoding ignores the existence of AN at the eavesdroppers, i.e. using the $\gamma_{\mathrm{E},mk}$ in (5.5d). This is a worst case approximation, since $\gamma_{\mathrm{E},mk}^{\mathrm{AN}}\leq\gamma_{\mathrm{E},mk}$. Moreover, the optimization problem uses all power which is not utilized for user signals for the transmission of AN, i.e. the PAPC in (5.5c) is forced to use all available power. The problem formulation is given by:

$$\min_{(\mathbf{t}_1,\ldots,\mathbf{t}_K,\mathbf{t}_a)} \quad \mathrm{tr}\left(\sum_{k=1}^{K}\mathbf{t}_k\mathbf{t}_k^{\mathrm{H}}\right) \tag{5.5a}$$

$$\text{subject to} \quad \frac{\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_k\right|^2}{\sum_{i\neq k}\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_i\right|^2+\left|\mathbf{h}_{\mathrm{B},k}^{\mathrm{H}}\mathbf{t}_a\right|^2+\sigma_{w_{\mathrm{B},k}}^2}\geq\gamma_{\mathrm{B},k,\min}, \quad \forall k, \tag{5.5b}$$

$$\left[\sum_{k=1}^{K}\mathbf{t}_k\mathbf{t}_k^{\mathrm{H}}+\mathbf{t}_a\mathbf{t}_a^{\mathrm{H}}\right]_{l,l}=1, \qquad \forall l, \tag{5.5c}$$

$$\frac{\left|\mathbf{h}_{\mathrm{E},m}^{\mathrm{H}}\mathbf{t}_k\right|^2}{\sum_{i\neq k}\left|\mathbf{h}_{\mathrm{E},m}^{\mathrm{H}}\mathbf{t}_i\right|^2+\sigma_{w_{\mathrm{E},m}}^2}\leq\gamma_{\mathrm{E},mk,\max}, \qquad \forall k,\forall m. \tag{5.5d}$$

The convex reformulation is equivalent to the normal SG precoding in Section 5.1.2. The matrix $\mathbf{T}_a = \mathbf{t}_a \mathbf{t}_a^{\mathrm{H}} \in \mathbb{C}^{L \times L}$ is defined which has to be positive semidefinite and the rank-one constraint is dropped to convexify the problem. The different strategies are evaluated in Section 5.2.1.

5.1.4 Selection of an Adaptive Coding and Modulation Scheme

A remaining problem is to find appropriate values for $\gamma_{\mathrm{B},k,\min}$ and $\gamma_{\mathrm{E},mk,\max}$ for the optimization process. It is not guaranteed that the optimization problem (5.3) is feasible for all SINR values due to the power limitation. In the DVB-S2X standard for SATCOM, an SINR value is given for each ACM scheme, such that a reliable BER performance is achieved [DVBS2X, Ch. 6]. Since secure channel coding schemes are derived from non-secure mother codes [KHM+11], it is possible to build a set of secure ACM schemes with associated SINR values for reliability $\gamma_{\mathrm{B,ACM}}$ and minimum security gap values $\gamma_{\mathrm{G,ACM}}$. In the following, fairness between all users is assumed, i.e. the data rate and security needs of all users are equal. However, in general, the SG precoding algorithm allows for different ACM schemes per user.

The algorithm to find a feasible ACM scheme for maximum secure data rate is shown in Fig. 5.1. In a nutshell, the ACM schemes are tested in decreasing order until a feasible one is found. The user's SINR value with ZF precoding is a good guess where to start the search. Moreover, due to CSI uncertainties, a reliability margin $\Delta\gamma_{\mathrm{B}}$, e.g. 1 dB, and a security margin $\Delta\gamma_{\mathrm{E}}$, e.g. 2 dB, may improve the robustness. If there are any matrices with $\mathrm{rank}(\mathbf{T}_k^*) > 1$, the suboptimal result of the Gaussian randomization process from Fig. 3.5 may lead to a reduced security gap. Hence, the process must test the achieved SINR values after a Gaussian randomization and continue with a lower ACM scheme in case of failure. Data encoded and modulated with the selected ACM scheme can now be transmitted securely with the resulting precoding vectors. For application of AN, the convex reformulation of (5.4) or (5.5) rather than (5.3) is used in the Algorithm 5.1.

5.2 Numerical Analysis

In this section, Monte-Carlo simulations are performed to evaluate the performance of the SG precoding algorithm. This includes the security gap performance with multiple eavesdroppers, different AN strategies and the secrecy region considering the scenario from Section 3.1.2. In general, a security gap $\gamma_{\mathrm{G,min}} = 5.00\,\mathrm{dB}$ is assumed for the simulations. Such a channel is enabled for secure communications with state-of-the-art channel codes [MOS22] including a small reliability and security margin. In contrast to

Data: ACM schemes (sorted by increasing SINR values)
Result: Precoding vectors $\mathbf{t}_k^*$
Compute ZF precoding with fairness objective (3.19)
Find index i_{ZF} of ACM schemes which SINR value is nearest to the SINR result of the ZF precoding
$i = i_{\mathrm{ZF}}$
repeat
  Get $\gamma_{\mathrm{B,ACM}}$ and $\gamma_{\mathrm{G,ACM}}$ from the nth ACM scheme
  Set $\gamma_{\mathrm{B},k,\min} = \gamma_{\mathrm{B,ACM}}\ \Delta\gamma_{\mathrm{B}}$
  Set $\gamma_{\mathrm{E},mk,\max} = \dfrac{\gamma_{\mathrm{B,ACM}}}{\gamma_{\mathrm{G,ACM}}\ \Delta\gamma_{\mathrm{E}}}$
  Compute optimization problem (5.3)
  if (5.3) *is solvable* **then**
    Set $\mathbf{T}_k^*$ to the solution of the optimization problem (5.3)
    Compute $\mathbf{t}_k^*$ with eigendecomposition or Gaussian randomization
    if $\mathbf{t}_k^*$ *achieve necessary SINR values* **then**
      Optimization is solved
    end
  end
  $i = i - 1$
until $i < 1$ *or optimization is solved*

Figure 5.1: ACM selection for the SG precoding.

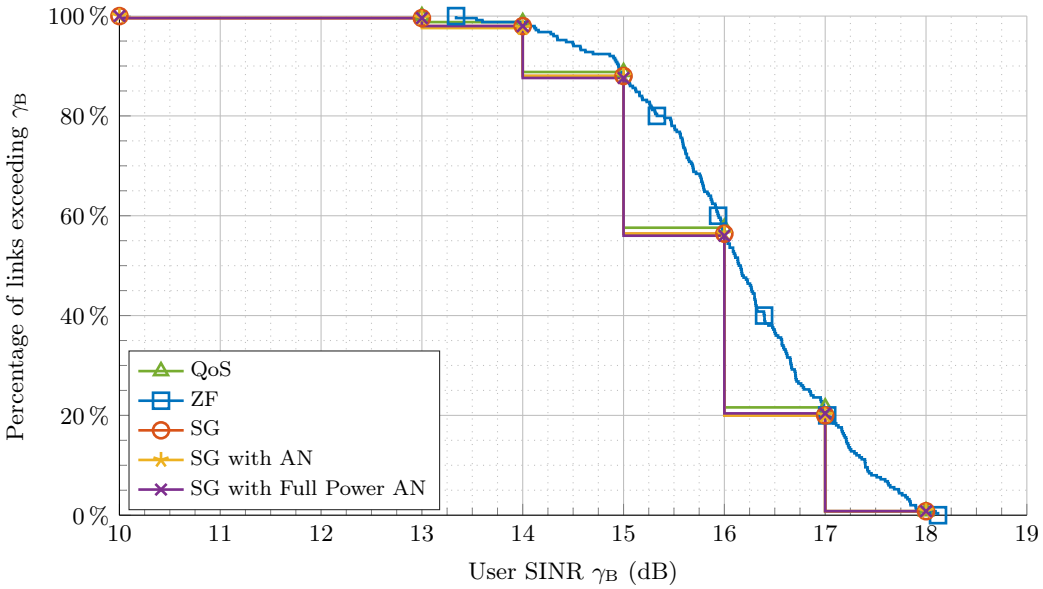

Figure 5.2: SG Precoding Performance: User SINR distribution for multiple user groups in case of $M = 2$ eavesdroppers

the numerical analysis on the MSC precoding in Chapter 4, the results of the SR antenna design are not shown in this section. This is due to the fact that powerful eavesdroppers are considered and, thus, the SG precoding is only feasible for about half of the user groups and provides poor performance for those.

5.2.1 Security Gap Performance

Before the security gap performance is analyzed, the achievable user SINR defines the ACM scheme for the transmission of data worth protecting. ACM schemes from 20 dB SINR down to 5 dB in steps of 1 dB are simulated applying the algorithm from Fig. 5.1. The ZF is expected to be an upper bound of the achievable SINR values for the QoS and the three variants of SG precoding. Even though the ZF precoding in Fig. 5.2 indicates higher SINR values, the ACM scheme which can be applied is in majority equal to the other evaluated precoding algorithms. In general, the user SINR is similar for all evaluated precoding algorithms with $M = 2$ eavesdroppers, with a minor diminution for the SG precoding variants. The single Monte-Carlo run (MCR) with a user SINR of 10 dB shown in Fig. 5.2 is due to a mischance of positioning of the users and eavesdroppers. The SG optimization problem is infeasible for higher SINR values. Separate these two users in the user grouping process may already resolve this issue.

The security gap performance of the SG precoding without and with both AN strategies

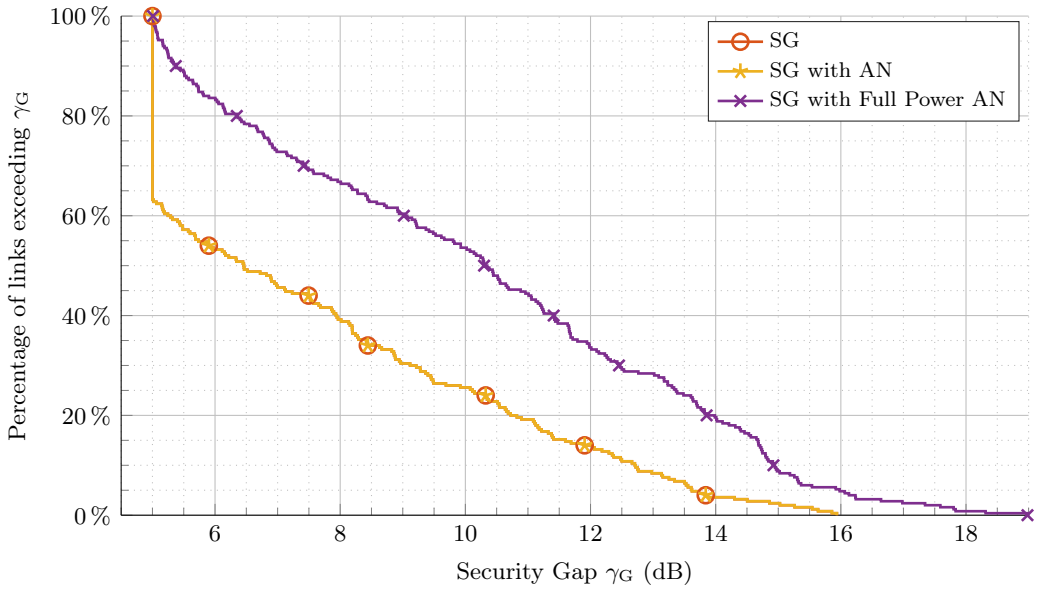

Figure 5.3: SG Precoding Performance: Security gap distribution for multiple user groups in case of $M = 2$ eavesdroppers

assuming $M = 2$ eavesdroppers is shown in Fig. 5.3. In all MCRs the three variants of SG precoding achieve the goal of $\gamma_{G,min} = 5.00\,\text{dB}$. The security gap levels of SG without AN and SG with AN from (5.4) are exactly equal and, thus, when the MIMO degrees of freedom are sufficient, i.e. $L \geq K + M$, this AN strategy does not provide any security gain. However, spending all unused power for AN, i.e. the SG with Full Power AN strategy, the security gap is improved for all user groups. If the security gap $\gamma_G > 5.00\,\text{dB}$, the SG precoding and SG precoding with AN are identical to the QoS precoding for these user groups. In these particular cases, even the QoS precoding algorithm from (5.1) allows secret transmission. Although this happens in 62 % of the MCRs, this is just luck due to the small number of eavesdroppers.

The user SINR distribution in Fig. 5.4 for ZF and QoS is the same in case of $M = 8$ eavesdroppers as it is for $M = 2$ eavesdroppers. This is not a surprise, since the algorithms are unaware of eavesdroppers. The user SINR values of the SG precoding algorithms, however, are decreased. For 2.4 % of the MCRs the SG precoding without AN and for a single user group the SG with AN variants, the optimization is infeasible, i.e. not able to achieve $\gamma_G = 5.00\,\text{dB}$. This single user group where the SG precoding with AN is infeasible is the same as the worst case of the MSC precoding in Section 4.2.2, i.e. one user and the 7th eavesdropper are only 4 km apart.

Evaluating the security gap performance in Fig. 5.5, the SG with Full Power AN is

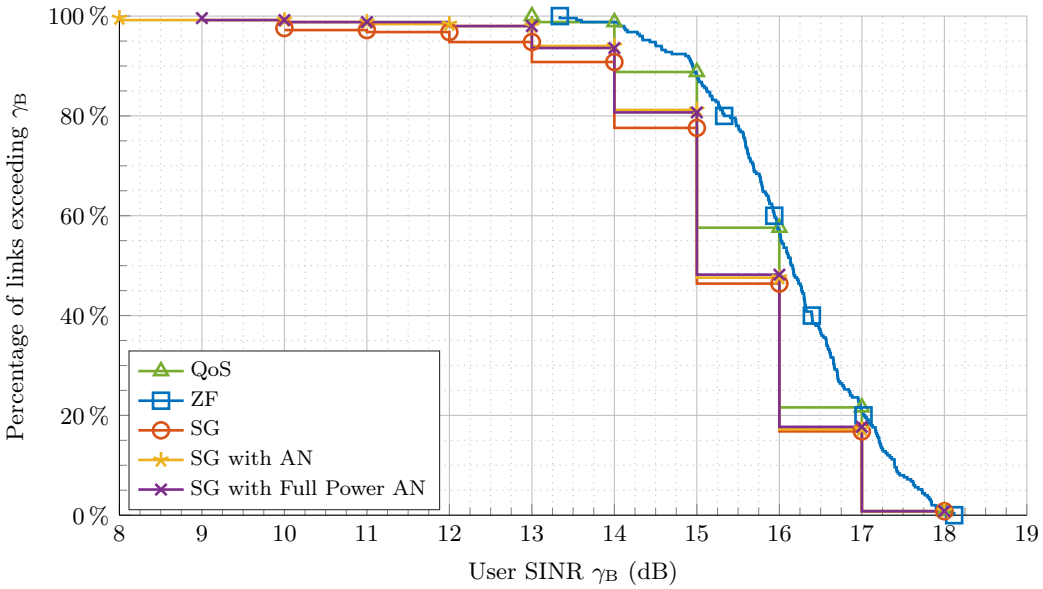

Figure 5.4: SG Precoding Performance: User SINR distribution for multiple user groups in case of $M = 8$ eavesdroppers

still leading. The SG without and with AN perform roughly equivalent, despite the fact that without AN the precoding fails in 2.4 % and otherwise only in a single MCR, and achieve exactly $\gamma_G = 5.00\,\text{dB}$ in about 80 % of the user groups. The non-secure ZF and QoS precoding cannot compete anymore in terms of security gap performance. For 30 % of the user groups, the eavesdropper intercepts the user signals with a higher SINR than the users.

Table 5.1 summarizes the average security gap $\mathrm{E}[\gamma_G]$, the average user SINR performance $\mathrm{E}[\gamma_B]$ (or $\mathrm{E}\left[\gamma_B^{AN}\right]$, respectively), as well as the average power usage of the simulations in dependency of the number of eavesdroppers. For the SG with Full Power AN, 96 % of the positive semidefinite matrices are rank-one. The SG with AN precoding is a special case where the AN precoding matrices are often high rank. However, if the AN precoding matrices are high rank, their trace, i.e. the power utilized for AN, is always close to zero and AN is unnecessary to solve the problem. For example, AN is not necessary for $M = 2$ eavesdroppers. Thus, in Table 5.1 the average AN power is only computed when the AN is necessary with an additional percentage for the probability of that condition. In general, the conversion to the precoding vector of a high rank SDP solution with the Gaussian randomization process is suboptimal. However, the number of constraints with many eavesdroppers in consideration prevents the guarantee of rank-one solutions.

In conclusion, the SG with Full Power AN brings the best security performance with a

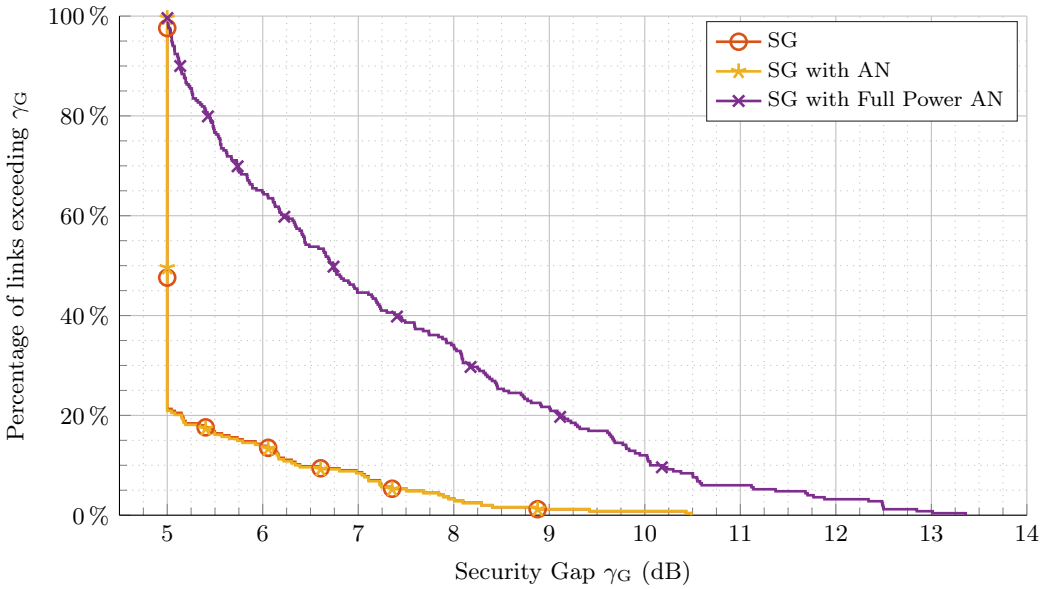

Figure 5.5: SG Precoding Performance: Security gap distribution for multiple user groups in case of $M = 8$ eavesdroppers

minor loss in user SINR in general. If $L \geq K + M$, the SG without AN is also sufficient and more energy efficient. The SG with AN precoding algorithm, however, is a middle course between energy-efficiency and performance when $L \leq K + M$.

5.2.2 Secrecy Region

The secrecy region gives insight into the areas where the security gap γ_G is above the predefined 5.00 dB threshold to guarantee secure data transmission for the users. The principle is equivalent to the secrecy region of the MSC precoding in Section 4.2.3. The areas in which this target value is not achieved, i.e. $\gamma_G \leq 5.00\,\text{dB}$, by applying the SG with Full Power AN are illustrated by blue color for the user B_1 and by orange color for B_2 in Fig. 5.6. Every receiver inside these areas can potentially decode the secure messages of the respective user. Keep in mind that the VR plots assume powerful eavesdroppers equipped with a receiver with +6 dB/K G/T relative to the UTs. Even if potential eavesdroppers install huge dish antennas to achieve an enormous receiver G/T of 37.5 dB/K instead of the typically assumed 25.5 dB/K, the VR only slightly increases which is shown in comparison of Fig. 4.6 (a) and (b). The eight eavesdropper locations are indicated by E_1 to E_8 which are all outside the colored areas in both eavesdropper G/T configurations. Hence, the eavesdroppers are not able to intercept the user signals with an SINR higher than $\gamma_B^{AN} - \gamma_G$ whereas for this particular user group in Fig. 5.6 the

Table 5.1: SG Precoding Performance and Power Usage with Multiple Eavesdroppers

Eves	**SG**	**SG with AN**	**SG with Full Power AN**	**QoS**	**ZF**
	Average Security Gap E[γ_G]				
$M = 2$	7.73 dB	7.73 dB	10.26 dB		
$M = 4$	6.38 dB	6.38 dB	8.61 dB		
$M = 8$	5.36 dB	5.36 dB	7.30 dB		
	Average User SINR E[γ_B]				
				15.68 dB	16.15 dB
$M = 2$	15.62 dB	15.62 dB	15.62 dB		
$M = 4$	15.58 dB	15.59 dB	15.59 dB		
$M = 8$	15.34 dB	15.38 dB	15.38 dB		

	Average Power Usage (% of total available power)						
	User	User	AN	User	AN	User	User
						83.5 %	100 %
$M = 2$	83.5%	83.5%	0.0% (0%)	84.1%	15.9%		
$M = 4$	83.1%	83.1%	2.1% (4%)	83.9%	16.1%		
$M = 8$	80.2%	80.9%	18.0% (15%)	82.5%	17.5%		

$\gamma_B^{AN} = 14.00\,\text{dB}$.

5.3 Summary

In this chapter, a precoding algorithm for the security gap metric is investigated. Since channel coding for PLS in Gaussian wiretap channels is still a challenging problem, the security gap is a high potential metric for practical implementations. Therefore, the optimization problem to maintain a certain security gap is derived from a QoS precoding constrained by a per-antenna power limit necessary for the considered HTS scenario. The SINR values for users and eavesdroppers are nonconvex and, thus, the problem is reformulated. To utilize efficient off-the-shelf numerical optimization methods, the common SDR technique is applied. Leveraging AN improves the security with the drawback of a higher power consumption at the transmitter, whereas two different AN strategies are presented. An iterative algorithm selects an ACM scheme for which the SG precoding optimization is feasible. Data encoded and modulated with the selected ACM scheme can be transmitted securely with the resulting precoding vectors.

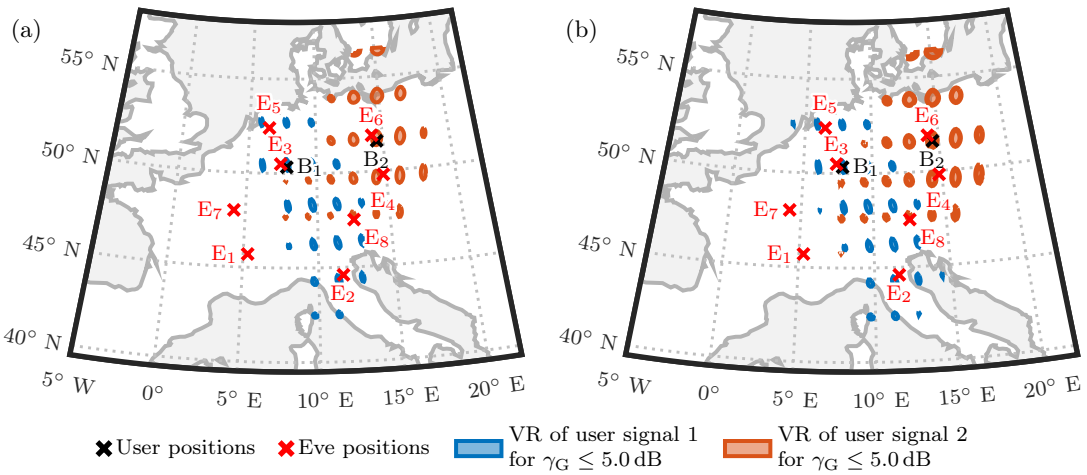

Figure 5.6: Vulnerability regions of the security gap with $M = 8$ eavesdroppers comprising a receiver with (a) +6 dB/K and (b) +18 dB/K relative to the default UTs

The numerical analysis is provided for the MR antenna design assuming state-of-the-art channel codes for key-less PLS. The optimization problem is feasible only for about half of the user groups if the single reflector is considered. In combination with the outcomes of the simulations with an MR antenna design, this again demonstrates the advantages of multiple reflector antennas on the satellite. The user SINR performance is approximately equal to the non-secure ZF and QoS precoding schemes. If the sum of the number of eavesdroppers and number of user is higher than the number of beams, i.e. the spatial degrees of freedom are not sufficient to achieve the requested security gap, the application of AN is helpful. The most critical aspect is the distance of receiver terminals. Since the LOS MIMO channels are very similar for users and eavesdroppers close together, it is delicate to distinguish them and, hence, the SG precoding may fail due to a reduced security gap. The VRs are small areas randomly distributed and mainly depending on the user positions. Hence, it is impossible for an eavesdropper to find a single position which allows the interception of all user groups.

6 Conclusion

6.1 All the Way to Implementations

Each year a few new GEO HTSs are launched with continuously increasing throughput or dimensions. For example, the *EUTELSAT KONNECT VHTS* launched in September 2022 is the largest GEO communications satellite with the highest throughput ever built in Europe [Tha22]. Moreover, some new HTSs, e.g. the *Avanti HYLAS-4* [Ava22], offer a few steerable beams, i.e. the beam center position can be modified by the operator after the launch of the satellite. The FR4 pattern is still commonly applied to minimizes the interference between neighboring beams. Although most of them employ an MR antenna design, based on the photographs of the satellites, the details on the design of the transponders and feeds are usually company confidential. It depends on the payload of the satellite if it is possible to illuminate a few neighboring beams in a FFR pattern. Hence, none of the contemporary HTSs can be utilized directly for practical tests of the secure precoding algorithms proposed in this thesis. Since transparent transponders in the satellite payload are sufficient for secure precoding, a practical test with an active HTS is possible if a satellite with MR antenna design and neighboring beams with FFR is found. However, an active cooperation with an HTS operator will be necessary to perform the tests.

Software-defined radios have become the industry standard in markets such as electronic warfare, test and measurement, or spectrum monitoring. The advances in integrated circuits for digital signal processing or analog-to-digital converters enable the implementation of SATCOM transceivers (transmitters and receivers) with use of software-defined radios. Software-defined radios were utilized in the testbed and field trial presented in [SSK20] to generate the precoded transmit signals and the estimation of the CSI at the two receivers. A pure software implementation of the secure precoding algorithms proposed in this thesis will suffice for a small scale field trial with a few beams, users, and eavesdroppers. Besides the precoding algorithms, the channel coding for security, e.g. punctured LDPC codes, and the modulation scheme can be implemented in software as well. However, the signal bandwidth will be restricted to a few MHz. In general, an

experimental setup implementing the gateway and UTs with software-defined radios is possible and can be analogous to the setup in [SSK20].

In advance of a practical test of the secure precoding algorithms, the estimation of the CSI of the eavesdroppers based on their positions should be practically evaluated. Since no satellite employing an MR antenna design and FFR is in the orbit, two neighboring beams with RHCP and LHCP signals on the same carrier frequency illuminated by different reflectors can be utilized, e.g. signals from the *Viasat KA-SAT*. Terminals with a linear polarized feed can receive both signals interfering each other[1] and, thus, behave like a receiver in the FFR scheme. Multiple UTs in the coverage area of those two beams measure their CSI and act as reference. Applying the reference CSI to the simulation model of the communications system results in an estimated CSI for a certain position. A CSI measurement of another receiver terminal at the respective position and the comparison with the estimated CSI validates the theory. Additionally, an automatic process to detect the position of eavesdroppers simplifies the applicability of the proposed algorithms. Machine learning algorithms can be trained to detect objects in satellite imagery [Van18; KTOW22]. Detecting satellite dish antennas of a critical size, e.g. approximately 4 m in the scenario of this thesis, could provide initial candidates of possible eavesdroppers.

In general, large-scale precoding for HTS systems is an open research problem [PVS+19]. Although there are fast interior-point algorithms available to solve SDP problems, e.g. the one presented in [JKL+20], the computational costs are still challenging for HTS systems with hundreds of beams. Moreover, splitting the uplink to the satellite over multiple gateways[2] necessitates interconnection and causes latency due to the exchange of CSI feedback and precoding vectors which may be computed centrally.

6.2 Conclusion

As SATCOM downlinks are broadcast channels by nature, it is rather easy for eavesdroppers to intercept user signals. This work aimed to increase the key-less PLS in geostationary satellite systems. In contrast to existing literature, the potentials and benefits of an MR antenna scheme has been investigated. For key-less PLS in wiretap channels, it is crucial that the legitimate users receive the signals in higher quality than all eavesdroppers. In this thesis, two precoding algorithms for PLS for SATCOM based on suitable secrecy metrics were proposed to generate such channel conditions to make PLS in SATCOM possible. Since multiple antennas on a satellite unlock the space

[1] Receiving RHCP and LHCP signals with a linear feed results in a sum signal of both components where the polarization mismatch impairs each circular signal by 3 dB.

[2] These gateways should be geographically separated to ensure high availability [Del19].

domain as a further physical resource, huge secrecy gains have been achieved compared to the achievable secrecy with an SR design. By additionally considering AN signals, the precoding algorithms were able to cover the case where the number of eavesdroppers exceeded the number of available beams and still achieved secrecy in the MR scenario. In conclusion, the results of this thesis demonstrate that the MR antenna design and FFR pattern provide a large step forward in making PLS for SATCOM practically achievable.

List of Operators and Symbols

List of Operators and Notation

x	a scalar
X	a random variable, set, event, etc. taken in context
$\mathbf{x} \in \mathbb{R}^m$	a length-m vector of real numbers
$\mathbf{A} \in \mathbb{C}^{m \times n}$	an $m \times n$ matrix of complex numbers
$n \in \mathbb{N}_0$	n is a natural number (integer) including 0
$\mathbf{A}^{\mathrm{H}}$	conjugate transpose of the matrix $\mathbf{A}$
$\mathbf{A}^{\mathrm{T}}$	transpose of the matrix $\mathbf{A}$
$\mathbf{A} \succeq 0$	matrix $\mathbf{A}$ is positive semidefinite
$\mathrm{diag}(\,\cdot\,)$	diagonal operator
$\mathrm{tr}(\mathbf{A})$	trace of the matrix $\mathbf{A}$
$\mathrm{rank}(\mathbf{A})$	rank of the matrix $\mathbf{A}$
$\lvert a \rvert$	absolute value of the scalar a
$\arg(a)$	argument (phase) of complex number a
$\lVert \mathbf{A} \rVert$	Euclidean norm of the matrix $\mathbf{A}$
$[\mathbf{a}]_m$	mth element of the vector $\mathbf{a}$
$[\mathbf{A}]_{m,n}$	entry of the matrix $\mathbf{A}$ at row m and column n
$\exp(x)$	exponential function e^x
$J_a(b)$	Bessel function of the first kind, order a and argument b
$\Pr(X)$	probability of an event X
$p_X(x)$	probability mass function of the discrete random variable X
$\mathrm{E}[X]$	expectation of the random variable X
σ_X^2	variance of the random variable X

σ_X	standard deviation of the random variable X
$\mathbf{x} \sim \mathcal{CN}(\mu, \Sigma)$	random vector $\mathbf{x}$ following a complex circular Gaussian distribution with mean μ and covariance Σ
$\mathrm{H}(X)$	entropy of the random variable X
$\mathrm{H}(X\|Y)$	conditional entropy of X given random variable Y, also called the equivocation of X about Y
$\mathrm{I}(X;Y)$	mutual Information of X relative to Y

List of Symbols

e	Euler's number
$\mathrm{j} = \sqrt{-1}$	imaginary unit
$\mathbf{I}_M$	identity matrix of dimension $M \times M$
$\mathrm{c}_0 = 299\,792\,458\,\mathrm{m/s}$	speed of light in vacuum
$K, K_\mathrm{T}, K_\mathrm{G}$	number of users (per group), total number of users, number of groups
L_R, L	number of satellite reflectors and number of illuminated beams
M	number of eavesdroppers
B, k	index and counting variable for users
E, m	index and counting variable for eavesdroppers
l_R, l, n, j, i	counting variables
$J_\mathrm{max}, I_\mathrm{max}$	maximum number of iterations
t, T_S	time and symbol period
x_l	transmit signal of the lth beam
s_k	modulated data signal of the kth user
$\mathbf{t}_k$	precoding vector for the kth user data signal
$h_{\mathrm{B},kl}, h_{\mathrm{E},ml}$	channel coefficient in beam l to user k and eavesdropper m
$\mathbf{h}_{\mathrm{B},k}, \mathbf{h}_{\mathrm{E},m}$	channel coefficient vector of user k and eavesdropper m

$w_{\mathrm{B},k}, w_{\mathrm{E},m}$	noise contribution at the user terminal k and eavesdropper terminal m
$a, \mathbf{t}_a$	AN signal, AN precoding vector
$y_{\mathrm{B},k}, y_{\mathrm{E},m}$	receive signal of user k, receive signal of eavesdropper m
$\gamma_{\mathrm{B},k}, \gamma_{\mathrm{B},k}^{\mathrm{AN}}$	receive SINR of user k, without and with AN
$\gamma_{\mathrm{E},mk}, \gamma_{\mathrm{E},mk}^{\mathrm{AN}}$	SINR of eavesdropper m to receive user data stream k, without and with AN
$g = a\,\mathrm{e}^{\mathrm{j}\varphi}$	complex gain comprising a power a and phase φ part
λ_c, f_c	carrier wavelength, carrier frequency
θ_{kl}	off-axis angle from point of boresight of beam l and user k
D_{S}	diameter of the satellite reflector array
$D_{l_{\mathrm{R}}}$	diameter of the satellite reflector l_{R}
$\mathbf{r}_l, \mathbf{r}_k, \mathbf{r}_m$	position of the feed l, UT k, and eavesdropper m
d_{kl}	radio path length from feed l to UT k
$\Delta\varphi$	phase error
$\mathbf{T}_k$	matrix for SDR reformulation of optimization problems
$\epsilon, \epsilon_{\mathrm{O}}, \epsilon_{\mathrm{S}}$	threshold or solution accuracy
$\mathbf{T}_k^*, \mathbf{t}_k^*$	globally optimal solution of SDR matrix and precoding vector
$\mathbf{T}_k^{\circledast}, \mathbf{t}_k^{\circledast}$	locally optimal or suboptimal solution of SDR matrix and precoding vector
$C_{\mathrm{B}}, C_{\mathrm{E}}$	user capacity, eavesdropper capacity
$C_S, C_{S,\min}$	secrecy capacity, minimum secrecy capacity
$\gamma_{\mathrm{B},\min}, \gamma_{\mathrm{E},\max}$	reliability SINR threshold, security SINR threshold
$p_e^{\mathrm{B}}, p_e^{\mathrm{E}}$	user BER, eavesdropper BER
$p_{e,\max}^{\mathrm{B}}, p_{e,\min}^{\mathrm{E}}$	reliability BER threshold, security BER threshold
γ_{G}	security gap
$c_{\min}, s_k, n_k, s_m, n_{mk}$	auxiliary variables for convex optimization

$\tilde{n}_k, \tilde{s}_m$	first-order Taylor approximation of auxiliary variables
$\mathbf{T}_k^{(0)}, \mathbf{t}_k^{(0)}$	initial feasible solutions for an optimization problem
$\mathbf{T}_k^{\circledast(j)}, \tilde{n}_k^{(j)}, \tilde{s}_m^{(j)}, c_{\min}^{(j)}$	variables during the jth iteration step

Acronyms

Alice	legitimate transmitter
Bob	legitimate receiver
Eve	aware passive adversary
Mallory	malicious active attacker
ACM	adaptive coding and modulation
AES	advanced encryption standard
AN	artificial noise
AWGN	additive white Gaussian noise
BER	bit-error rate
CCI	co-channel interference
CCP	convex-concave procedure
CFO	carrier frequency offset
CSI	channel state information
DCP	disciplined convex programming
DMWC	discrete memoryless wiretap channel
ECC	error correction code
FDD	frequency-division duplexing
FDMA	frequency-division multiple access
FFR	full frequency reuse
FR4	four-color frequency reuse
FSP	free space propagation
FSS	fixed satellite service

G/T	gain-to-noise-temperature
GEO	geostationary Earth orbit
GNSS	global navigation satellite system
HPA	high power amplifier
HTS	high throughput satellite
IoT	internet of things
LDPC	low density parity check
LEO	low Earth orbit
LHCP	left-hand circular polarization
LO	local oscillator
LOS	line-of-sight
MAC	message authentication code
MADOC	multiple antenna downlink orthogonal clustering
MCR	Monte-Carlo run
ME	multiple eavesdropper
MIMO	multiple-input multiple-output
MISO	multiple-input single-output
MR	multiple-reflector
MSC	minimum secrecy capacity
MU-MIMO	multiuser MIMO
PAPC	per-antenna power constraint
PLA	physical layer authentication
PLKG	physical layer key generation
PLS	physical layer security
QoS	quality of service
RHCP	right-hand circular polarization
RSA	Rivest-Shamir-Adleman
RSS	received signal strength

SATCOM	satellite communications
SDP	semidefinite programming
SDR	semidefinite relaxation
SEE	secrecy energy efficiency
SFPB	single feed per beam
SG	security gap
SIC	successive interference cancellation
SINR	signal-to-interference-plus-noise ratio
SISO	single-input single-output
SNR	signal-to-noise ratio
SOP	secrecy outage probability
SR	single-reflector
SVD	singular value decomposition
TDD	time-division duplexing
UAV	unmanned aerial vehicle
UT	user terminal
VR	vulnerability region
ZF	zero-forcing

List of Tables

List of Figures

Bibliography

[AAE23] N. Abdelsalam, S. Al-Kuwari, and A. Erbad, *Physical Layer Security in Satellite Communication: State-of-the-art and Open Problems*, arXiv, 2023-01. DOI: 10.48550/ARXIV.2301.03672.

[AC93] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing", *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993. DOI: 10.1109/18.243431.

[All11] J. E. Allnutt, *Satellite-to-Ground Radiowave Propagation*, ser. Electromagnetic Waves. Institution of Engineering and Technology, 2011, p. 681, ISBN: 9781849191500. DOI: 10.1049/PBEW054E.

[ALYZ18] K. An, T. Liang, X. Yan, and G. Zheng, "On the Secrecy Performance of Land Mobile Satellite Communication Systems", *IEEE Access*, vol. 6, pp. 39 606–39 620, 2018. DOI: 10.1109/ACCESS.2018.2854233.

[Ava22] Avanti Communications, "HYLAS Fleet Specifications", 2022-11. [Online]. Available: https://www.avanti.space/wp-content/uploads/2022/11/HYLAS-Fleet-Specifications_November-2022.pdf.

[BBC12] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding With Scrambling, Concatenation, and HARQ for the AWGN Wire-Tap Channel: A Security Gap Analysis", *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 883–894, 2012. DOI: 10.1109/TIFS.2012.2187515.

[BD06] 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.

[BHT15] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-Control Coding for Physical-Layer Secrecy", *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1725–1746, 2015. DOI: 10.1109/JPROC.2015.2463678.

[BLJJ20] K.-L. Besser, P.-H. Lin, C. R. Janda, and E. A. Jorswieck, "Wiretap Code Design by Neural Network Autoencoders", *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3374–3386, 2020. DOI: 10.1109/TIFS.2019.2945619.

[BOO09] F. Bohagen, P. Orten, and G. E. Oien, "On spherical vs. plane wave modeling of line-of-sight MIMO channels", *IEEE Transactions on Communications*, vol. 57, no. 3, pp. 841–849, 2009. DOI: 10.1109/TCOMM.2009.03.070062.

[BV04] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004. DOI: 10.1017/CBO9780511804441.

[CJL+16] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, *Report on Post-Quantum Cryptography*, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, 2016-04. DOI: 10.6028/NIST.IR.8105.

[CK78] I. Csiszar and J. Korner, "Broadcast channels with confidential messages", *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978. DOI: 10.1109/TIT.1978.1055892.

[CQ19] H. Chen and C. Qi, "User Grouping for Sum-Rate Maximization in Multiuser Multibeam Satellite Communications", in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–6. DOI: 10.1109/ICC.2019.8761875.

[DBN+01] M. Dworkin, E. Barker, J. Nechvatal, J. Foti, L. Bassham, E. Roback, and J. Dray, *Advanced Encryption Standard (AES)*, Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD, 2001-11. DOI: 10.6028/NIST.FIPS.197.

[Del19] T. Delamotte, "MIMO Feeder Links for Very High Throughput Satellite Systems", Ph.D. dissertation, Universität der Bundeswehr München, 2019.

[DH76] W. Diffie and M. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976. DOI: 10.1109/TIT.1976.1055638.

[DKA+21] M. T. Damir, A. Karrila, L. Amorós, O. W. Gnilke, D. Karpuk, and C. Hollanti, "Well-Rounded Lattices: Towards Optimal Coset Codes for Gaussian and Fading Wiretap Channels", *IEEE Transactions on Information Theory*, vol. 67, no. 6, pp. 3645–3663, 2021. DOI: 10.1109/TIT.2021.3059749.

[DSS+21] T. Delamotte, M. G. Schraml, R. T. Schwarz, K.-U. Storek, and A. Knopp, "Multi-Antenna-Enabled 6G Satellite Systems: Roadmap, Challenges and Opportunities", in *WSA 2021; 25th International ITG Workshop on Smart Antennas*, 2021, pp. 1–6.

[DVBS2X] ETSI EN 302 307-2 (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; Part 2: DVB-S2 Extensions (DVB-S2X)", European Telecommunications Standards Institute, Standard, 2021.

[FFWL21] Q.-Y. Fu, Y.-H. Feng, H.-M. Wang, and P. Liu, "Initial Satellite Access Authentication Based on Doppler Frequency Shift", *IEEE Wireless Communications Letters*, vol. 10, no. 3, pp. 498–502, 2021. DOI: 10.1109/LWC.2020.3035811.

[FHA21] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "New Physical Layer Key Generation Dimensions: Subcarrier Indices/Positions-Based Key Generation", *IEEE Communications Letters*, vol. 25, no. 1, pp. 59–63, 2021. DOI: 10.1109/LCOMM.2020.3025262.

[FSW19] R. Fritschek, R. F. Schaefer, and G. Wunder, "Deep Learning for the Gaussian Wiretap Channel", in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–6. DOI: 10.1109/ICC.2019.8761681.

[FTA+16] H. Fenech, A. Tomatis, S. Amos, V. Soumpholphakdy, and J. L. Serrano Merino, "Eutelsat HTS systems", *International Journal of Satellite Communications and Networking*, vol. 34, no. 4, pp. 503–521, 2016-07. DOI: 10.1002/sat.1171.

[FWH19] H. Fang, X. Wang, and L. Hanzo, "Learning-Aided Physical Layer Authentication as an Intelligent Process", *IEEE Transactions on Communications*, vol. 67, no. 3, pp. 2260–2273, 2019. DOI: 10.1109/TCOMM.2018.2881117.

[GAZ+20] K. Guo, K. An, B. Zhang, Y. Huang, X. Tang, G. Zheng, and T. A. Tsiftsis, "Physical Layer Security for Multiuser Satellite Communication Systems With Threshold-Based Scheduling Scheme", *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5129–5141, 2020. DOI: 10.1109/TVT.2020.2979496.

[GB08] M. Grant and S. Boyd, "Graph implementations for nonsmooth convex programs", in *Recent Advances in Learning and Control*, ser. Lecture Notes in Control and Information Sciences, V. Blondel, S. Boyd, and H. Kimura, Eds., Springer-Verlag Limited, 2008, pp. 95–110.

[GB20] ——, *CVX: Matlab Software for Disciplined Convex Programming, version 2.2*, http://cvxr.com/cvx, 2020.

[GBY06] M. Grant, S. Boyd, and Y. Ye, "Disciplined Convex Programming", in *Global Optimization: From Theory to Implementation*. Boston, MA: Springer US, 2006, pp. 155–210, ISBN: 978-0-387-30528-8. DOI: 10.1007/0-387-30528-9_7.

[GLE08] P. K. Gopala, L. Lai, and H. El Gamal, "On the Secrecy Capacity of Fading Channels", *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008. DOI: 10.1109/TIT.2008.928990.

[GN08] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise", *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008. DOI: 10.1109/TWC.2008.060848.

[HBJL18] Y. Hu, S. Bian, B. Ji, and J. Li, "GNSS Spoofing Detection Technique Using Fraction Parts of Double-difference Carrier Phases", *Journal of Navigation*, vol. 71, no. 5, pp. 1111–1129, 2018. DOI: 10.1017/S0373463318000206.

[HFA19] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey", *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2019. DOI: 10.1109/COMST.2018.2878035.

[HFGV19] W. K. Harrison, T. Fernandes, M. A. C. Gomes, and J. P. Vilela, "Generating a Binary Symmetric Channel for Wiretap Codes", *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 2128–2138, 2019. DOI: 10.1109/TIFS.2019.2892010.

[HM09] W. K. Harrison and S. W. McLaughlin, "Physical-Layer Security: Combining Error Control Coding and Cryptography", in *2009 IEEE International Conference on Communications*, 2009, pp. 1–5. DOI: 10.1109/ICC.2009.5199337.

[HN21] W. Henkel and M. Namachanja, "A Simple Physical-Layer Key Generation for Frequency-Division Duplexing (FDD)", in *2021 15th International Conference on Signal Processing and Communication Systems (ICSPCS)*, 2021, pp. 1–6. DOI: 10.1109/ICSPCS53099.2021.9660264.

[HP10] Y. Huang and D. P. Palomar, "Rank-Constrained Separable Semidefinite Programming With Applications to Optimal Beamforming", *IEEE Transactions on Signal Processing*, vol. 58, no. 2, pp. 664–678, 2010. DOI: 10.1109/TSP.2009.2031732.

[HSSK16] C. Hofmann, K.-U. Storek, R. T. Schwarz, and A. Knopp, "Spatial MIMO over satellite: A proof of concept", in *2016 IEEE International Conference on Communications (ICC)*, 2016, pp. 1–6. DOI: 10.1109/ICC.2016.7510945.

[HX04] K. Ho and W. Xu, "An accurate algebraic solution for moving source location using TDOA and FDOA measurements", *IEEE Transactions on Signal Processing*, vol. 52, no. 9, pp. 2453–2463, 2004. DOI: 10.1109/TSP.2004.831921.

[JKL+20] H. Jiang, T. Kathuria, Y. T. Lee, S. Padmanabhan, and Z. Song, "A Faster Interior Point Method for Semidefinite Programming", in *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, 2020, pp. 910–918. DOI: 10.1109/FOCS46700.2020.00089.

[JUN05] M. Joham, W. Utschick, and J. Nossek, "Linear transmit processing in MIMO communications systems", *IEEE Transactions on Signal Processing*, vol. 53, no. 8, pp. 2700–2712, 2005. DOI: 10.1109/TSP.2005.850331.

[KHM+11] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC Codes for the Gaussian Wiretap Channel", *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 532–540, 2011. DOI: 10.1109/TIFS.2011.2134093.

[KSL13] A. Knopp, R. T. Schwarz, and B. Lankl, "Secure MIMO SATCOM Transmission", in *MILCOM 2013 - 2013 IEEE Military Communications Conference*, 2013, pp. 284–288. DOI: 10.1109/MILCOM.2013.56.

[KTOW22] J. Kang, S. Tariq, H. Oh, and S. S. Woo, "A Survey of Deep Learning-Based Object Detection Methods and Datasets for Overhead Imagery", *IEEE Access*, vol. 10, pp. 20 118–20 134, 2022. DOI: 10.1109/ACCESS.2022.3149052.

[KW10a] A. Khisti and G. W. Wornell, "Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel", *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, 2010. DOI: 10.1109/TIT.2010.2048445.

[KW10b] ——, "Secure Transmission With Multiple Antennas—Part II: The MIMOME Wiretap Channel", *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, 2010. DOI: 10.1109/TIT.2010.2068852.

[LAL19] W. Lu, K. An, and T. Liang, "Robust Beamforming Design for Sum Secrecy Rate Maximization in Multibeam Satellite Systems", *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 3, pp. 1568–1572, 2019. DOI: 10.1109/TAES.2019.2905306.

[LB16] T. Lipp and S. Boyd, "Variations and extension of the convex-concave procedure", *Optimization and Engineering*, vol. 17, pp. 263–287, 2016-06. DOI: 10.1007/s11081-015-9294-x.

[LCMC11] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-Based Transmit Beamforming in the Presence of Eavesdroppers: An Optimized Artificial-Noise-Aided Approach", *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1202–1216, 2011. DOI: 10.1109/TSP.2010.2094610.

[LFZZ20] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-Layer Security in Space Information Networks: A Survey", *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 33–52, 2020. DOI: 10.1109/JIOT.2019.2943900.

[LH78] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel", *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978. DOI: 10.1109/TIT.1978.1055917.

[LHVH11] J. Lei, Z. Han, M. Á. Vazquez-Castro, and A. Hjorungnes, "Secure Satellite Communication Systems Design With Individual Secrecy Rate Constraints", *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 661–671, 2011. DOI: 10.1109/TIFS.2011.2148716.

[LLBS14] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, "Semantically Secure Lattice Codes for the Gaussian Wiretap Channel", *IEEE Transactions on Information Theory*, vol. 60, no. 10, pp. 6399–6416, 2014. DOI: 10.1109/TIT.2014.2343226.

[LLO+19] Z. Lin, M. Lin, J. Ouyang, W.-P. Zhu, A. D. Panagopoulos, and M.-S. Alouini, "Robust Secure Beamforming for Multibeam Satellite Communication Systems", *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 6202–6206, 2019. DOI: 10.1109/TVT.2019.2913793.

[LMS+10] Z.-q. Luo, W.-k. Ma, A. M.-c. So, Y. Ye, and S. Zhang, "Semidefinite Relaxation of Quadratic Optimization Problems", *IEEE Signal Processing Magazine*, vol. 27, no. 3, pp. 20–34, 2010. DOI: 10.1109/MSP.2010.936019.

[LSR+20] I. Leyva-Mayorga, B. Soret, M. Röper, D. Wübben, B. Matthiesen, A. Dekorsy, and P. Popovski, "LEO Small-Satellite Constellations for 5G and Beyond-5G Communications", *IEEE Access*, vol. 8, pp. 184 955–184 964, 2020. DOI: 10.1109/ACCESS.2020.3029620.

[LW16] H. Li and X. Wang, "Detection of GPS spoofing through signal multipath signature analysis", in *2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, 2016, pp. 1–5. DOI: 10.1109/CCECE.2016.7726713.

[LYO+19] Z. Lin, C. Yin, J. Ouyang, X. Wu, and A. D. Panagopoulos, "Robust Secrecy Energy Efficient Beamforming in Satellite Communication Systems", in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–5. DOI: 10.1109/ICC.2019.8761056.

[LZT+22] C. Li, H. Zhu, J. Tang, J. Hu, and G. Li, "User Grouping in Multiuser Satellite MIMO Downlink With Fairness Consideration", *IEEE Wireless Communications Letters*, vol. 11, no. 8, pp. 1575–1579, 2022. DOI: 10.1109/LWC.2022.3165807.

[Mau93] U. Maurer, "Secret key agreement by public discussion from common information", *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993. DOI: 10.1109/18.256484.

[MBH09] N. Marina, R. Bose, and A. Hjørungnes, "Increasing the secrecy capacity by cooperation in wireless networks", in *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2009, pp. 1978–1982. DOI: 10.1109/PIMRC.2009.5450066.

[MBS20] G. Maral, M. Bousquet, and Z. Sun, *Satellite Communications Systems: Systems, Techniques and Technology*. John Wiley & Sons, Ltd, 2020-04, p. 792, ISBN: 9781119382089. DOI: 10.1002/9781119673811.

[MOS22] T. Matsumine, H. Ochiai, and J. Shikata, "Security Gap Improvement of BICM Systems Through Bit-Labeling Optimization for the Gaussian Wiretap Channel", *IEEE Access*, vol. 10, pp. 47 805–47 813, 2022. DOI: 10.1109/ACCESS.2022.3172481.

[MV11] H. Mahdavifar and A. Vardy, "Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes", *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428–6443, 2011. DOI: 10.1109/TIT.2011.2162275.

[MvOV97] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1997, p. 810. DOI: 10.1201/9780429466335.

[MWM19] J. M. McGinthy, L. J. Wong, and A. J. Michaels, "Groundwork for Neural Network-Based Specific Emitter Identification Authentication for IoT", *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6429–6440, 2019. DOI: 10.1109/JIOT.2019.2908759.

[NLS12] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-Efficient Resource Allocation for Secure OFDMA Systems", *IEEE Transactions on Vehicular Technology*, vol. 61, no. 6, pp. 2572–2585, 2012. DOI: 10.1109/TVT.2012.2199145.

[OH08] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel", in *2008 IEEE International Symposium on Information Theory*, 2008, pp. 524–528. DOI: 10.1109/ISIT.2008.4595041.

[PDW19] T. Peng, W. Dai, and M. Z. Win, "Efficient and Robust Physical Layer Key Generation", in *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*, 2019, pp. 1–6. DOI: 10.1109/MILCOM47813.2019.9020770.

[PF22] J. Pfeiffer and R. F. Fischer, "Multilevel Coding for Physical-Layer Security", *IEEE Transactions on Communications*, vol. 70, no. 3, pp. 1999–2009, 2022. DOI: 10.1109/TCOMM.2022.3145578.

[PVS+19] A. I. Perez-Neira, M. A. Vazquez, M. B. Shankar, S. Maleki, and S. Chatzinotas, "Signal Processing for High-Throughput Satellites: Challenges in New Interference-Limited Scenarios", *IEEE Signal Processing Magazine*, vol. 36, no. 4, pp. 112–131, 2019. DOI: 10.1109/MSP.2019.2894391.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978-02. DOI: 10.1145/359340.359342.

[RTL98] F. Rashid-Farrokhi, L. Tassiulas, and K. R. Liu, "Joint optimal power control and beamforming in wireless networks using antenna arrays", *IEEE Transactions on Communications*, vol. 46, no. 10, pp. 1313–1324, 1998. DOI: 10.1109/26.725309.

[Sch19] R. Schwarz, "MIMO Satellite Communications for Fixed Satellite Services", Ph.D. dissertation, Universität der Bundeswehr München, 2019.

[SDSK19] R. T. Schwarz, T. Delamotte, K.-U. Storek, and A. Knopp, "MIMO Applications for Multibeam Satellites", *IEEE Transactions on Broadcasting*, vol. 65, no. 4, pp. 664–681, 2019. DOI: 10.1109/TBC.2019.2898150.

[Sha48] C. E. Shannon, "A mathematical theory of communication", *The Bell System Technical Journal*, vol. 27, no. 4, pp. 623–656, 1948. DOI: 10.1002/j.1538-7305.1948.tb00917.x.

[Sha49] ——, "Communication theory of secrecy systems", *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949. DOI: 10.1002/j.1538-7305.1949.tb00928.x.

[SHK15a] K.-U. Storek, C. A. Hofmann, and A. Knopp, "Impact of the Atmosphere on the Signal Phase and the Channel Capacity in EHF MIMO Satellite Links", in *2015 IEEE Global Communications Conference (GLOBECOM)*, 2015, pp. 1–7. DOI: 10.1109/GLOCOM.2015.7417384.

[SHK15b] ——, "Measurements of phase fluctuations for reliable MIMO space communications", in *2015 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob)*, 2015, pp. 157–162. DOI: 10.1109/APWiMob.2015.7374956.

[Sho97] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997. DOI: 10.1137/S0097539795293172.

[SK17a] M. G. Schraml and A. Knopp, "Blind Estimation of the HPA Operating Point in Multicarrier Satellite Transponders", *IEEE Communications Letters*, vol. 21, no. 5, pp. 1051–1054, 2017. DOI: 10.1109/LCOMM.2017.2653118.

[SK17b] ——, "Cumulant based operating point estimation for communication satellite transponders", in *2017 IEEE International Conference on Communications (ICC)*, 2017, pp. 1–7. DOI: 10.1109/ICC.2017.7996646.

[SK17c] K.-U. Storek and A. Knopp, "Fair User Grouping for Multibeam Satellites with MU-MIMO Precoding", in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, 2017, pp. 1–7. DOI: 10.1109/GLOCOM.2017.8255098.

[SK20] M. G. Schraml and A. Knopp, "Physical Layer Security with Unknown Eavesdroppers in Beyond-5G MU-MIMO SATCOM", in *2020 IEEE 3rd 5G World Forum (5GWF)*, 2020, pp. 180–185. DOI: 10.1109/5GWF49715.2020.9221107.

[SK22] ——, "Precoding for Security Gap Physical Layer Security in Multiuser MIMO Satellite Systems", in *MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM)*, 2022, pp. 612–617. DOI: 10.1109/MILCOM55135.2022.10017639.

[SKS19] M. G. Schraml, A. Knopp, and K.-U. Storek, "Multi-User MIMO Satellite Communications with Secrecy Constraints", in *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*, 2019, pp. 17–22. DOI: 10.1109/MILCOM47813.2019.9020847.

[SSH04] Q. Spencer, A. Swindlehurst, and M. Haardt, "Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels", *IEEE Transactions on Signal Processing*, vol. 52, no. 2, pp. 461–471, 2004. DOI: 10.1109/TSP.2003.821107.

[SSK20] K.-U. Storek, R. T. Schwarz, and A. Knopp, "Multi-Satellite Multi-User MIMO Precoding: Testbed and Field Trial", in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–7. DOI: 10.1109/ICC40277.2020.9148757.

[SSK21] M. G. Schraml, R. T. Schwarz, and A. Knopp, "Multiuser MIMO Concept for Physical Layer Security in Multibeam Satellite Systems", *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1670–1680, 2021. DOI: 10.1109/TIFS.2020.3040884.

[ST12] W. L. Stutzmann and G. A. Thiele, *Antenna Theory and Design*. John Wiley & Sons, Inc., 2012, p. 848, ISBN: 978-0-470-57664-9.

[Tha22] Thales Alenia Space. (2022-09-08). "EUTELSAT KONNECT VHTS communications satellite successfully launched", [Online]. Available: https://www.thalesgroup.com/en/worldwide/space/press-release/eutelsat-

konnect - vhts - communications - satellite - successfully - launched (visited on 2023-02-09).

[TKY21] O. A. Topal, G. K. Kurt, and H. Yanikomeroglu, "Securing the Inter-Spacecraft Links: Physical Layer Key Generation From Doppler Frequency Shift", *IEEE Journal of Radio Frequency Identification*, vol. 5, no. 3, pp. 232–243, 2021. DOI: 10.1109/JRFID.2021.3077756.

[TMV+21] L. Torres-Figueroa, U. J. Mönich, J. Voichtleitner, A. Frank, V.-C. Andrei, M. Wiese, and H. Boche, "Experimental Evaluation of a Modular Coding Scheme for Physical Layer Security", in *2021 IEEE Global Communications Conference (GLOBECOM)*, 2021, pp. 1–6. DOI: 10.1109/GLOBECOM46510.2021.9685785.

[TV05] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005. DOI: 10.1017/CBO9780511807213.

[Van18] A. Van Etten, *You Only Look Twice: Rapid Multi-Scale Object Detection In Satellite Imagery*, arXiv, 2018-05. DOI: 10.48550/ARXIV.1805.09512.

[VH19] Á. Vázquez-Castro and M. Hayashi, "Physical Layer Security for RF Satellite Channels in the Finite-Length Regime", *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 981–993, 2019. DOI: 10.1109/TIFS.2018.2868538.

[WBZH19] D. Wang, B. Bai, W. Zhao, and Z. Han, "A Survey of Optimization Approaches for Wireless Physical Layer Security", *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1878–1911, 2019. DOI: 10.1109/COMST.2018.2883144.

[WES08] A. Wiesel, Y. C. Eldar, and S. Shamai, "Zero-Forcing Precoding and Generalized Inverses", *IEEE Transactions on Signal Processing*, vol. 56, no. 9, pp. 4409–4418, 2008. DOI: 10.1109/TSP.2008.924638.

[WGHE18] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS Signal Authentication Via Power and Distortion Monitoring", *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 2, pp. 739–754, 2018. DOI: 10.1109/TAES.2017.2765258.

[WKX+18] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead", *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018. DOI: 10.1109/JSAC.2018.2825560.

[WSKK18] S. P. Winter, M. G. Schraml, M. T. Knopp, and A. Knopp, "Spatial Modulation for Improved Eavesdropping Resistance in Multi-Beam Satellite Downlinks", in *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, 2018, pp. 829–834. DOI: 10.1109/MILCOM.2018.8599822.

[Wyn75] A. D. Wyner, "The wire-tap channel", *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975. DOI: 10.1002/j.1538-7305.1975.tb02040.x.

[WZY+20] Z. Wu, Y. Zhang, Y. Yang, C. Liang, and R. Liu, "Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey", *IEEE Access*, vol. 8, pp. 165 444–165 496, 2020. DOI: 10.1109/ACCESS.2020.3022294.

[YAZ+22] P. Yue, J. An, J. Zhang, G. Pan, S. Wang, P. Xiao, and L. Hanzo, *On the Security of LEO Satellite Communication Systems: Vulnerabilities, Countermeasures, and Future Trends*, arXiv, 2022-01. DOI: 10.48550/ARXIV.2201.03063.

[YG06] T. Yoo and A. Goldsmith, "On the optimality of multiantenna broadcast scheduling using zero-forcing beamforming", *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 3, pp. 528–541, 2006. DOI: 10.1109/JSAC.2005.862421.

[YVS15] P. L. Yu, G. Verma, and B. M. Sadler, "Wireless physical layer authentication via fingerprint embedding", *IEEE Communications Magazine*, vol. 53, no. 6, pp. 48–53, 2015. DOI: 10.1109/MCOM.2015.7120016.

[ZAO12] G. Zheng, P.-D. Arapoglou, and B. Ottersten, "Physical Layer Security in Multibeam Satellite Systems", *IEEE Transactions on Wireless Communications*, vol. 11, no. 2, pp. 852–863, 2012. DOI: 10.1109/TWC.2011.120911.111460.

[ZDMW16] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key Generation From Wireless Channels: A Review", *IEEE Access*, vol. 4, pp. 614–626, 2016. DOI: 10.1109/ACCESS.2016.2521718.

[Zen15] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities", *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, 2015. DOI: 10.1109/MCOM.2015.7120014.

[ZLZ+22] X. Zhang, G. Li, J. Zhang, A. Hu, Z. Hou, and B. Xiao, "Deep-Learning-Based Physical-Layer Secret Key Generation for FDD Systems", *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6081–6094, 2022. DOI: 10.1109/JIOT.2021.3109272.

[ZWZ+21] P. Zimmer, R. Weinreich, C. T. Zenger, A. Sezgin, and C. Paar, "Keys from the Sky: A First Exploration of Physical-Layer Security Using Satellite Links", in *ICC 2021 - IEEE International Conference on Communications*, 2021, pp. 1–7. DOI: 10.1109/ICC42927.2021.9500958.