Physical Layer Security in Massive MIMO Systems

by

Jun Zhu

M. A. Sc., University of Victoria, 2011
B. Sc., Southeast University, 2008

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

in

The Faculty of Graduate and Postdoctoral Studies

(Electrical and Computer Engineering)

THE UNIVERSITY OF BRITISH COLUMBIA
(Vancouver)

June 2016

Abstract

Massive multiple-input multiple-output (MIMO) is one of the key technologies for the emerging fifth generation (5G) wireless networks, and has the potential to tremendously improve spectral and energy efficiency with low-cost implementations. While massive MIMO systems have drawn great attention from both academia and industry, few efforts have been made on how the richness of the spatial dimensions offered by massive MIMO affects wireless security. As security is crucial in all wireless systems due to the broadcast nature of the wireless medium, in this thesis, we study how massive MIMO technology can be used to guarantee communication security in the presence of a passive multi-antenna eavesdropper. Our proposed massive MIMO system model incorporates relevant design choices and constraints such as time-division duplex (TDD), uplink training, pilot contamination, low-complexity signal processing, and low-cost hardware components. The thesis consists of three main parts.

We first consider physical layer security for a massive MIMO system employing simple artificial noise (AN)-aided matched-filter (MF) precoding at the base station (BS). For both cases of perfect training and pilot contamination, we derive a tight analytical lower bound for the achievable ergodic secrecy rate, and an upper bound for the secrecy outage probability. Both bounds are expressed in closed form, providing an explicit relationship between all system parameters, offering significant insights for system design.

We then generalize the work by comparing different types of linear data and AN precoders in a secure massive MIMO network. The system performance, in terms of the achievable ergodic secrecy rate is obtained in closed form. In addition, we propose a novel low-complexity data and AN precoding strategy based on a matrix polynomial expansion.

Finally, we consider a more realistic system model by taking into account non-ideal hardware components. Based on a general hardware impairment model, we derive a lower bound for the ergodic secrecy rate achieved by each user when AN-aided MF precoding is employed at the BS. By exploiting the derived analytical bound, we investigate the impact of various system parameters on the secrecy rate and optimize both the uplink training pilots and AN precoder to maximize the secrecy rate.

Preface

Chapters 2–4 are based on works under the supervision of Professor Robert Schober and Professor Vijay K. Bhargava.

For all chapters, I conducted the paper survey on related topics, formulated the problems, proposed problem solutions, and performed the analysis and the simulations of the considered communication systems. I also wrote all paper drafts.

Two papers related to Chapter 2 have been published:

- J. Zhu, R. Schober, and V. K. Bhargava, “Secure transmission in multicell massive MIMO systems,” *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 4766–4781, Sept. 2014.

- J. Zhu, R. Schober, and V. K. Bhargava, “Secure transmission in multi-cell massive MIMO systems,” in *Proceedings of IEEE Global Telecommunications Conference (Globecom 2013) Workshop*, Atlanta, GA, Dec. 2013.

Three papers related to Chapter 3 have been published:

- J. Zhu, R. Schober, and V. K. Bhargava, “Linear precoding of data and artificial noise in secure massive MIMO systems,” *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.

- J. Zhu, R. Schober, and V. K. Bhargava, “Secrecy analysis of multi-cell massive MIMO systems with RCI precoding and artificial noise transmission,” in *Pro-*

ceedings of IEEE International Symposium on Communications, Control, and Signal Processing 2014 (ISCCSP'14), Athens, Greece, May 2014.

- J. Zhu, R. Schober, and V. K. Bhargava, "Secure downlink transmission in massive MIMO system with zero-forcing precoding," in *Proceedings of IEEE European Wireless 2014 (EW'14)*, Barcelona, Spain, May 2014.

Two papers related to Chapter 4 have been submitted:

- J. Zhu, D. W. K. Ng, N. Wang, R. Schober, and V. K. Bhargava, "Analysis and design of secure massive MIMO systems in the presence of hardware impairments," submitted to possible journal, Feb. 2016.

- J. Zhu, R. Schober, and V. K. Bhargava, "Physical layer security for massive MIMO systems impaired by phase noise," in *Proceedings of IEEE International workshop on Signal Processing advances in Wireless Communications 2016 (SPAWC 2016)*, Edinburgh, UK, July 2016.

Table of Contents

Appendices

List of Tables

List of Figures

List of Abbreviations

5G	5th Generation
3GPP	3rd Generation Partnership Project
LTE	(3GPP) Long Term Evolution
LTE-A	(3GPP) Long Term Evolution - Advanced
CDMA	Code Division Multiple Access
MIMO	Multiple–Input Multiple–Output
MISO	Multiple–Input Single–Output
SISO	Single–Input Single–Output
AWGN	Additive White Gaussian Noise
BS	Base Station
MT	Mobile Terminal
AN	Artificial Noise
NS	Null Space
PHY	Physical Layer
MAC	Media Access Control
CDF	Cumulative Distribution Function
PDF	Probability Distribution Function
r.v.	Random Variable
CSI	Channel State Information
DPC	Dirty Paper Coding

FDD	Frequency Division Duplex
i.i.d.	Independent and Identically Distributed
MAC	Medium Access Control
MMSE	Minimum Mean Squared Error
ZF	Zero-Forcing
RCI	Regularized Channel-Inversion
MF	Matched-Filter
POLY	Polynomial
MSE	Mean Squared Error
RF	Radio Frequency
SIC	Successive Interference Cancellation
SINR	Signal–to–Interference–plus–Noise Ratio
SNR	Signal–to–Noise Ratio
TDD	Time Division Duplex
w.r.t.	With Respect to
PA	Power Amplifier
CE	Constant Envelope
SO	Spatially Orthogonal
TO	Temporally Orthogonal

Notation

$(\cdot)^T$	Transpose
$(\cdot)^H$	Hermitian transpose
$\mathbf{0}$	All–zero column vector
$\mathbf{1}$	All–one column vector
$\mathbf{I}$	Identity matrix
$\mathbb{Z}^+$	The set of positive integer
$\mathbb{C}$	The set of complex number
$\mathbb{C}^{m\times n}$	The space of all $m \times n$ matrices with complex-valued elements
$\mathbb{E}[\cdot]$	Expectation operator
$\mathrm{var}(\cdot)$	Variance operator
$\|\| \cdot \|\|^2$	Euclidean norm operator
$\mathrm{diag}\{\mathbf{x}\}$	A diagonal matrix with the elements of vector $\mathbf{x}$ on the main diagonal
$\mathrm{tr}\{\cdot\}$	Trace of a matrix
$\mathrm{rank}\{\cdot\}$	Rank of a matrix
$\overline{X}$	Upper bound for X
$\underline{X}$	Lower bound for X
$\mathbb{CN}(\mathbf{0}, \mathbf{\Sigma})$	A circularly symmetric complex Gaussian random variable with zero mean and covariance matrix $\mathbf{\Sigma}$
χ_n^2	A chi-square random variable with n degrees of freedom
$[\,\cdot\,]_{kl}$	The element in the k^{th} row and l^{th} column of a matrix

$[\,\cdot\,]^+$	$\max\{0, x\}, \quad x \in \mathbb{R}$
$\lceil x \rceil$	The smallest integer no smaller than x
$\lfloor x \rfloor$	The largest integer no greater than x
$\lvert \mathcal{S} \rvert$	The cardinality of set $\mathcal{S}$

Acknowledgments

First and foremost I would like to express my deep and sincere gratitude to my supervisors, Professor Robert Schober and Professor Vijay K. Bhargava, for their patient guidance, encouragement, and invaluable advice throughout my time as their student. Both of them set great examples of being a distinguished researcher and excellent teacher. The knowledge and attitude I learned from them benefit me forever. I am thankful for the opportunity to work with them over the years. Without their support and guidance, this thesis would not be possible.

Also, I greatly thank the members of my doctoral committee, for their time and effort in evaluating my work and providing valuable feedback and suggestions.

Many thanks go to my dear laboratory colleagues at Lab Kaiser 4090 in Vancouver and IDC in Erlangen, research collaborators, and friends, for their presences and fun-loving spirits that made the otherwise grueling experience enjoyable.

Finally, I would like to thank the Natural Sciences and Engineering Research Council of Canada (NSERC), the University of British Columbia, the German Academic Exchange Service (DAAD), the Alexander von Humboldt Foundation, and the China Scholarship Council (CSC), not only for providing the funding which allowed me to undertake the research, but also for giving me the opportunity to attend conferences and meet so many interesting people in the world.

Dedication

To My Parents, Grandma, and Girlfriend Miss Xie Zhang

Chapter 1

Introduction

The fifth generation (5G) wireless system is expected to create a paradigm shift compared to the current Long Term Evolution (LTE)/LTE-Advanced systems in order to meet the unprecedented demands for future wireless applications, including the tremendous throughput and massive connectivity. Massive multiple-input multiple-output (MIMO) [1]-[8], an architecture employing large-scale multiuser MIMO processing using the array of hundreds or even thousands of antennas, simultaneously serving tens or hundreds of mobile users, has been identified as a promising air interface technology to address a significant portion of the above challenges. Besides, security is a vital issue in wireless networks due to the broadcast nature of the medium [10]. Despite the great efforts on massive MIMO from both academia and industry, the security paradigms guaranteeing the confidentiality of wireless communications in 5G networks have scarcely been stated. These motivate us to consider the massive MIMO system from the security perspective. This chapter provides an overview of a series of fundamentals related to this thesis, including massive MIMO, physical layer security, and hardware impairments.

The chapter is organized as follows. In Sections 1.1 and 1.2, we briefly review the fundamentals of ideal and non-ideal hardware constrained massive MIMO systems, respectively. In Section 1.3, we introduce the concept of physical layer security. In Section 1.4, we motivate the thesis by illustrating why we consider physical layer security in massive MIMO systems. The contributions conducted in this thesis are summarized in Section 1.5, and the thesis organization is provided in Section 1.6.

1.1 Massive MIMO Wireless Systems

Massive MIMO systems, also known as large-scale antenna or very large MIMO systems, equip base station (BS) antenna arrays with an order of magnitude more elements than what is used in current systems, i.e., a hundred antennas or more, and simultaneously serve low-complexity single-antenna mobile terminals (MTs) [1]-[8]. Massive MIMO enjoys all the benefits of conventional multiuser MIMO, such as improved data rate, reliability and reduced interference, but at a much larger scale and with simple linear precoding/detection schemes [1]-[3]. Remarkable improvements in rates as well as in spectral and power efficiency can be achieved by focusing the radiating power onto the MTs with the very large antenna array [6]. Massive MIMO is therefore capable of achieving robust performance at low signal-to-interference-plus-noise ratio (SINR) with highly efficient and inexpensive implementations, as the effects of noise and interference vanish completely in the limit of an infinite number of antennas [5]. Other benefits of massive MIMO include but are not limited to the extensive use of inexpensive low-power components, reduced latency, simplification of the media access control (MAC) layer, and robustness to intentional jamming [1]-[3]. This section will review the fundamentals of massive MIMO systems from the following perspectives: uplink pilot training in Section 1.1.1, downlink linear precoding in Section 1.1.2, and pilot contamination in Section 1.1.3.

1.1.1 Time-Division Duplex and Uplink Pilot Training

In this subsection, we review the operations for channel state information (CSI) acquisition applicable for massive MIMO systems. It is well understood that the

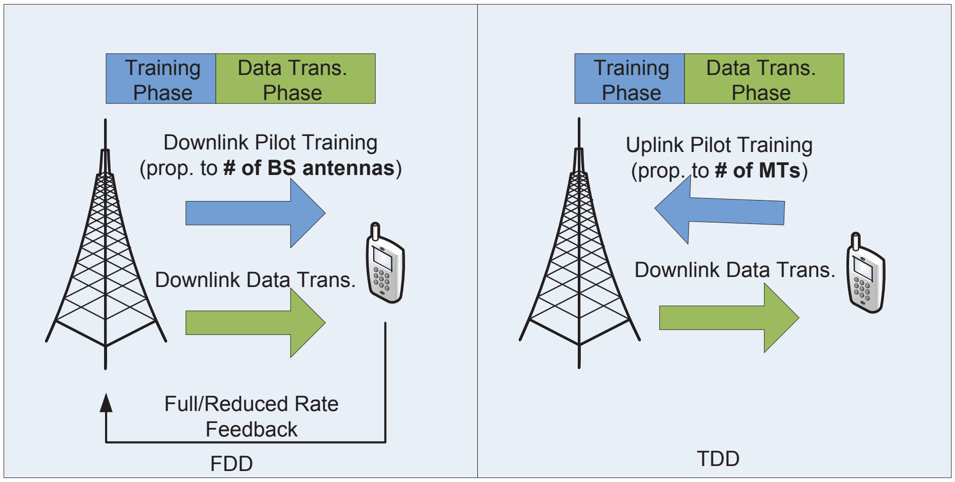

Figure 1.1: FDD mode versus TDD mode.

acquisition of CSI is essential for signal processing at the BS. Most current cellular systems work on frequency-division duplex (FDD) mode, where the CSI is typically acquired via feedback (full or limited) [11], as shown in Fig. 1.1. However, when the BS is equipped with large excess of antennas compared with the number of terminals, which is customary for massive MIMO systems, the time-division duplex (TDD) mode provides the only solution to acquire CSI. This is because the training burden for uplink pilots in a TDD system is proportional to the number of MTs, but independent of the number of BS antennas, while conversely the training burden for downlink pilots in an FDD system is proportional to the number of BS antennas [5]. The adoption of an FDD system imposes a severe limitation on the number of antennas deployed at the BS. By exploiting the reciprocity between uplink and downlink channels for TDD systems, the BS is able to eliminate the need for feedback, and uplink pilot training is sufficient for providing the desired uplink and downlink CSI.

1.1.2 Downlink Linear Precoding

With the desired downlink CSI available via uplink training by exploiting the channel reciprocity for TDD operation, the BS performs precoding in order to simultaneously serve multiple single-antenna MTs. Most precoding techniques are identical to those used for conventional multiuser MIMO schemes, but at a much larger scale. The theoretical sum-capacity optimal dirty paper coding (DPC) technique [12] is too complex to be implemented in practice even in a conventional MIMO system, and is thus not considered here. In contrast, linear precoding is typically adopted in massive MIMO systems. The most popular scheme is matched-filter (MF) precoding, due to its simple processing and robustness to CSI error [2, 5, 8]. However, MF precoding results in a performance degradation with increasing number of serving MTs. This is because when more MT channels exist, the near orthogonality between the MT channels becomes weak, which increases the level of multiuser interference. In this case, zero-forcing (ZF)/regularized channel inversion (RCI) precoding are preferable [13]-[15]. Like in the conventional MIMO system, the former suppresses the multiuser interference, while the latter strikes a balance between MF and ZF precoding. Unfortunately, they require high-dimensional matrix inversions, which lead to a high computational complexity, especially when the number of BS antennas and MTs are both large.

In order to reduce the computational complexity induced by conventional linear precoding techniques, e.g., ZF/RCI precoding in massive MIMO systems, the related literature has also investigated precoding schemes based on matrix polynomials, which avoids the need of large dimension matrix inversion calculations. The concept was originally conceived for code division multiple access (CDMA) uplink systems in [16] and later extended to MIMO systems in [17]. The main idea is to adopt matrix

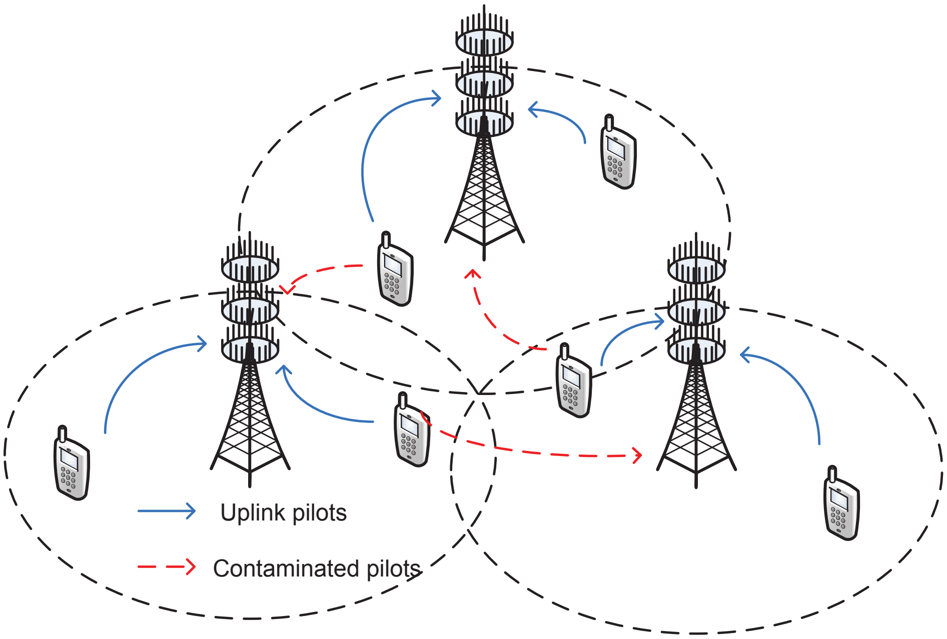

Figure 1.2: Pilot contamination in multi-cell massive MIMO systems.

polynomials with several terms to approximate matrix inversion. Thereby, the coefficients of the matrix polynomials need to be optimized in order to achieve a certain approximation accuracy.

1.1.3 Multi-Cell Deployment and Pilot Contamination

In massive MIMO systems, each terminal is ideally assigned to an orthogonal uplink pilot sequence. However, the maximum number of orthogonal pilot sequences are limited by the coherence block length. When deployed in a multi-cell network the available orthogonal pilot sequences are quickly exhausted. As such, pilot sequences have to be re-used from one cell to another. The negative effect incurred by the pilot re-use is generally called pilot contamination [1, 8], as shown in Fig. 1.2. More precisely, when the BS estimates the channel of a specific MT, it correlates the received pilot signal with the pilot sequence of that MT. In the case of pilot reuse between

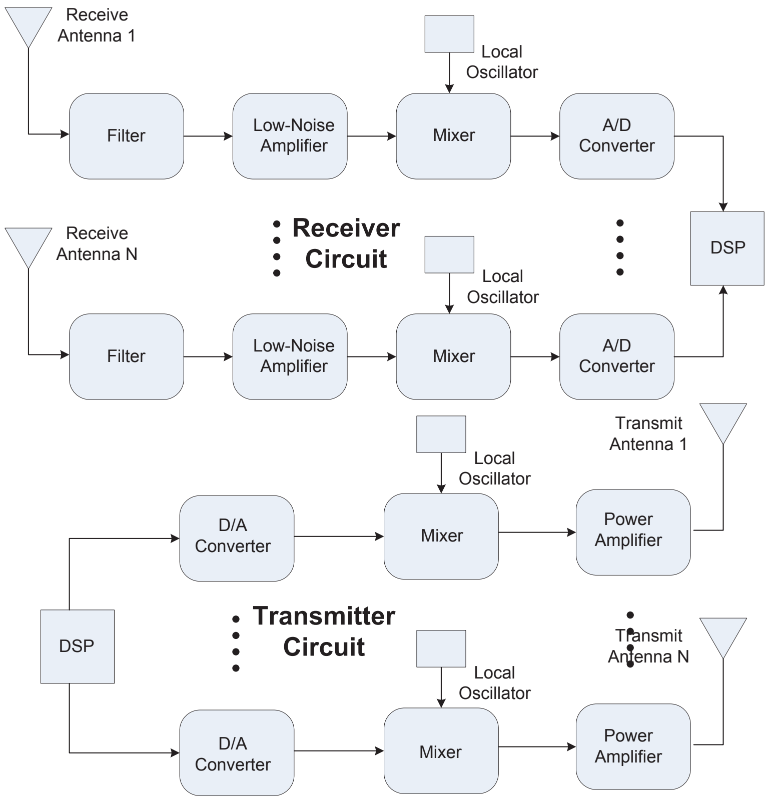

Figure 1.3: Transceiver hardware model.

cells, it actually acquires a channel estimate that is contaminated by a linear combination of channels associated with other MTs that share the same pilot sequence. The downlink precoding based on the contaminated channel estimates introduces interference which is directed to the MTs that share the same pilot sequence. The directed interference grows with the number of BS antennas at the same speed as the desired signal. Similar interference also exists for uplink data transmission.

1.2 Hardware Impairments in Massive MIMO Systems

Massive MIMO, as reviewed in Section 1.1, is able to bring substantial improvements in spectral and energy efficiency to wireless systems, due to the high spatial resolution and array gain provided by large-scale antenna arrays. Thus, massive MIMO has been identified as the promising air interface technology for 5G wireless networks. When the large-scale antenna array is deployed in practice, the hardware cost is a significant issue to address, as it scales linearly with the number of BS antennas [18], as shown in Fig. 1.3. In order to reduce the total expenditure, one solution is to adopt low-cost transceivers, in contrast to current expensive and high-quality circuit components. Unfortunately, such transceivers are usually prone to hardware imperfections, e.g., amplifier non-linearities, I/Q-imbalance, phase noise, and quantization errors [18]. Although such impairments can be mitigated by analog and digital signal processing techniques [19], they cannot be removed completely, due to the randomness introduced by different sources of imperfection. Transceiver implementations consist of various hardware components, including filters, converters, mixers, and amplifiers [18]. Each of them distorts the signals in a different manner. Generally speaking, non-ideal hardware components impair the transceiver by 1) introducing the mismatch between the intended transmit signal and what is actually emitted and 2) distorting the received signal in the reception processing. From the system performance perspective, instead of the individual behavior of each hardware component, the aggregate effects of all the residual hardware impairments is more important.

Among the literature, several works have investigated the impact of hardware impairments on massive MIMO systems [18], [20, 21, 22]. The impact of phase noise

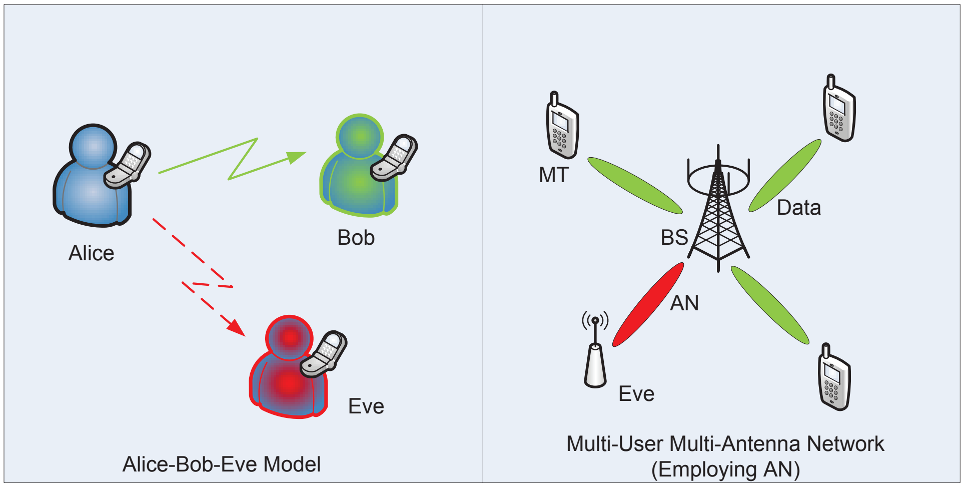

Figure 1.4: Physical layer security model.

originating from free-running oscillators on the downlink performance of massive MIMO systems was studied in [20] for different linear precoder designs. Constant envelope precoding for massive MIMO was studied in [21] with the objective of avoiding distortions caused by power amplifier nonlinearities at the transmitter. The impact of the aggregate effects of several hardware impairments originating from different sources on massive MIMO systems was studied in [18] by modelling the residual impairments remaining after compensation as additive distortion noises [19]. The authors in [22] presented closed-form expressions for the achievable user rates in uplink massive MIMO systems for a general residual hardware impairment model including both multiplicative phase noise and additive distortion noise.

1.3 Physical Layer Security

Security is a vital issue in wireless networks due to the broadcast nature of the medium. Traditionally, security has been achieved through cryptographic encryption implemented at the application layer, which requires a certain form of information (e.g., key) shared between the legitimate entities [9, 10]. This approach ignores the behavior of the communication channels and relies on the theoretical assumption that communication between the legitimate entities is error free. More importantly, all cryptographic measures assume that it is computationally infeasible for them to be deciphered without knowledge of the secret key, which remains mathematically unproven. Ciphers that were considered potentially unbreakable in the past are continually defeated due to the increasingly growth of computational power. Moreover, error free communication cannot be always guaranteed in non-deterministic wireless channels [10]. A novel approach for wireless security taking advantage of the characteristics of physical layer communication channels was proposed by Wyner in [23] and is referred to as physical layer security. The concept was originally developed for the classical wire-tap channel [23], cf. Fig. 1.4 (left). Wyner showed that a source (Alice)-destination (Bob) pair can exchange perfectly secure messages with a positive rate if the desired receiver enjoys better channel conditions than the eavesdropper (Eve). However, this condition cannot always hold in practice, especially in wireless fading channels. To make things worse, Eve enjoys a better average channel gain than Bob as long as he/she is located closer to Alice than Bob. Therefore, perfectly secure communication seems impossible, and techniques to enhance Bob's channel condition while degrading Eve's are needed. One option is to utilize artificial noise (AN) to perturb Eve's reception [24], as shown in Fig. 1.4 (right). Eves are typically passive so as to hide their existence, and thus their CSI cannot be obtained by Alice. In this case, multiple transmit antennas can be exploited to enhance secrecy by simultaneously transmitting both the information-bearing signal and AN. Specifically, precoding is used to make the AN invisible to Bob while degrading the decoding performance of possibly present Eves [24, 25]. In [26], authors investigated the secrecy outage probability for the AN-aided secrecy system, where only Alice has multiple antennas. When Eve is also equipped with multiple antennas, the work in [27] employs AN precoder to achieve a near-optimal performance in high signal-to-noise (SNR) regime. The contribution extends to a secrecy system where all nodes have multiple antennas in [28].

More recent studies have considered physical layer security provisioning in multiuser networks [29]-[36]. Although the secrecy capacity region for multiuser networks remains an open problem, it is interesting to investigate the achievable secrecy rates of such networks for certain practical transmission strategies. All aformentioned work generally assumed that Alice can acquire perfect CSI of Bob, which seems too ideal. Robust beamforming designs with estimated CSI were reported in [37]-[41]. Finally, the literature on physical layer security for the emerging massive MIMO systems will be discussed in Section 1.4.3.

1.4 Physical Layer Security in Massive MIMO Systems

The emerging massive MIMO architecture offers tremendous performance gains in terms of network throughput and energy efficiency by employing simple coherent processing on the large-scale antenna array. However, very little attention has been given to the security issue in massive MIMO systems. In order to address this concern, we need first to consider two fundamental questions: 1) Is massive MIMO secure? 2) If not, how can we improve security in massive MIMO systems? In this section, we illustrate the main motivation of this thesis by providing brief and general responses to the two questions.

1.4.1 Is Massive MIMO Secure?

Compared with conventional MIMO, massive MIMO is inherently more secure, as the large-scale antenna array equipped at the transmitter (Alice) can accurately focus a narrow and directional information beam on the intended terminal (Bob), such that the received signal power at Bob is several orders of magnitude higher than that at any incoherent passive eavesdropper (Eve) [42]. Unfortunately, this benefit may vanish if Eve also employs a massive antenna array for eavesdropping. The following scenarios further deteriorate the security of the massive MIMO system:

- As Eve is passive, it is able to move arbitrarily close to Alice without being detected by either Alice or Bob. In this case, the signal received by Eve can be strong.
- In a ultra-dense multi-cell network, Bob suffers from severe multiuser interference (both pilot contaminated and uncontaminated), while Eve may have access to the information of all other MTs, e.g., by collaborating with them, and remove their interference when decoding Bob's information.
- In practice, both Alice and Bob are equipped with low-cost transceivers to reduce the total expenditure, which are prone to hardware imperfections, while Eve has ideal hardware.

In the aforementioned scenarios, unless additional measures to secure the communication are taken by Alice, even a single passive Eve is able to intercept the signal intended for Bob [43]. Furthermore, we note that Eve could emit its own pilot symbols to impair the channel estimates obtained at Alice to improve his ability to decode Bob's signals during downlink transmission [44]. However, this would also increase the chance that the presence of the eavesdropper is detected by Alice [45]. Therefore, in this thesis, we limit ourselves to passive eavesdropping.

1.4.2 How to Improve Security for Massive MIMO?

Massive MIMO systems offer an abundance of BS antennas, while multiple transmit antennas can be exploited for secrecy enhancement, e.g., by emitting AN. Therefore, the combination of both concepts seems natural and promising. There arise several challenges and open problems for physical layer security provisioning in massive MIMO systems that are not present for conventional MIMO systems. We summarize them as follows.

- In a conventional massive MIMO system (without security), pilot contamination constitutes a limit on performance in terms of data throughput [5]. However, its effects on the AN design, as well as wireless security have not been considered.

- One of the tremendous advantages of massive MIMO in the physical layer is the simple processing, e.g., MF precoding. It remains unknown if more advanced and sophisticated signal processing techniques, e.g., ZF/RCI precoding and BS collaboration are beneficial in terms of data throughput and security, in a pilot contaminated environment.

- In conventional MIMO systems, AN is transmitted in the null space (NS) of the channel matrix [24]. The complexity associated with computing the NS may not be affordable in case of massive MIMO and thus simpler AN precoding methods are essential.

- When deployed in practice, low-cost transceivers are equipped to reduce the total expenditure. Such components are usually prone to hardware imperfections. The effects of the imperfections on the AN design, as well as the resulting security performance remains an open problem.

This thesis will provide detailed and insightful solutions to the aforementioned challenges and problems. As massive MIMO will serve as an essential enabling technology for the emerging 5G wireless networks, it is expected that its design from physical layer security perspective opens a new and promising research path. Related contributions will be summarized in Section 1.4.3.

1.4.3 Prior Arts

In this section, we summarize the related work on the topic of physical layer security for massive MIMO systems. In [46], the authors summarized the possible research options for the design of physical layer security in the emerging massive MIMO systems. Large system secrecy analysis of MIMO systems achieved by RCI precoding was provided in [47]-[49]. In [50], the authors adopted the channel between Alice and Bob as secrete key and showed that the complexity required by Eve to decode Alice's message is at least of the same order as a worst-case lattice problem. AN-aided jamming for Rician fading massive MIMO channels was investigated in [51], where the power allocation is optimized between messages and AN for both uniform and directional jamming. [52] investigated power scaling law for secure massive MIMO systems without the help of AN. The authors in [53] defined a new term *secrecy area* where all legitimate MTs satisfy the secrecy outage probability requirements within this area. An optimal power allocation strategy was performed to maximize this area. In the context of massive MIMO relaying, the work presented in [54] and [55] compared two classic relaying schemes, i.e., amplify-and forward (AF) and decode-and-forward (DF), for physical layer security with imperfect CSI at the massive MIMO relay. Authors in [56] provided a large system secrecy rate analysis for simultaneous wireless information and power transfer (SWIPT) MIMO wiretap channels. Whereas [51]-[56] and the contributions in this thesis all assumed that Eve is passive, the so-called pilot contamination attack [44], a form of active eavesdropping, was also considered in the literature. In particular, several techniques for detection of the pilot contamination attack were proposed in [42], including a detection scheme based on random pilots and a cooperative detection scheme. Moreover, the authors in [57] developed a secret key agreement protocol under the pilot contamination attack, and the authors in [58] proposed to encrypt the pilot sequence in order to hide it from the attacker. The encryption enables the MTs to achieve the performance as if they were under no attack. Methods for combating the pilot contamination attack in a multi-cell network was reported in [59], which exploited the low-rank property of the transmit correlation matrices of massive MIMO channels.

1.5 Contributions of the Thesis

This is the first thesis considering physical layer security in massive MIMO systems. In this thesis, we study secure downlink transmission in single/multi-cell massive MIMO systems in the presence of a multi-antenna eavesdropper which attempts to intercept the signal intended for any one of the MTs. To arrive at an achievable secrecy rate for this MT, we assume that the eavesdropper can acquire perfect knowledge of the CSI of all user data channels and is able to cancel all interfering MT signals. Ergodic secrecy rate and secrecy outage probability are the two performance evaluation metrics adopted in this thesis. The research work is divided into three chapters. The contributions in each chapter are as follows:

1. **AN-aided MF precoding**: Chapter 2 presents the first study of physical layer

security in pilot contaminated massive MIMO systems. In this chapter, we derive tight lower bounds for the ergodic secrecy rate and tight upper bounds for the secrecy outage probability for both cases of perfect training and pilot contamination, when BS employs simple MF precoding and AN precoding. The derived bounds are in closed form and provide significant insight for system design. In particular, the obtained results allow us to predict under what conditions (i.e., for what number of BS antennas, eavesdropper antennas, users, path-loss, number of cells, and pilot power) a positive secrecy rate is possible. Furthermore, we show that employing random AN precoding matrices is an attractive low-complexity option for massive MIMO systems. We also derive a closed-form expression for the fraction of transmit power that should be optimally allocated to AN and show that, for a given number of BS antennas, this fraction increases with the number of eavesdropper antennas and decreases with the number of users in the system. The work in Chapter 2 was published in [43, 60].

2. **Linear data and AN precoding**: Chapter 3 studies the performance-complexity tradeoff of selfish and collaborative data and AN precoders. Selfish precoders require only the CSI of the MTs in the local cell but cause inter-cell interference and inter-cell AN leakage. In contrast, collaborative precoders require the CSI between the local BS and the MTs in all cells, but reduce inter-cell interference and inter-cell AN leakage. However, since the additional CSI required for the collaborative precoders can be estimated directly by the local BS, the additional overhead and complexity incurred compared to selfish precoders is limited. We then derive novel closed-form expressions for the asymptotic ergodic secrecy rate which facilitate the performance comparison of different combinations of linear

data precoders (i.e., MF, selfish and collaborative ZF/RCI) and AN precoders (i.e., random, selfish and collaborative NS), and provide significant insight for system design and optimization. In order to avoid the computational complexity and potential stability issues in fixed point implementations entailed by the large-scale matrix inversions required for ZF and RCI data precoding and NS AN precoding, we propose polynomial (POLY) data and AN precoders and optimize their coefficients. We borrow the tools from free probability theory [61] to obtain the POLY coefficients. This allows us to express the POLY coefficients as simple functions of the channel and system parameters. Simulation results reveal that these precoders are able to closely approach the performance of selfish RCI data and NS AN precoders, respectively. The work in Chapter 3 was published in [62, 63, 64].

3. **AN-aided MF precoding with hardware imperfections**: Chapter 4 presents the first study of physical layer security in hardware constrained massive MIMO systems. For the adopted generic residual hardware impairment model, we derive a tight lower bound for the ergodic secrecy rate achieved by a downlink user when MF data precoding is employed at the massive MIMO BS. The derived bound provides insight into the impact of various system and channel parameters, such as the phase noise variance, the additive distortion noise parameters, the AN precoder design, the amount of power allocated to the AN, the pilot sequence design, the number of deployed local oscillators (LOs), and the number of users, on the ergodic secrecy rate. As conventional NS AN precoding is sensitive to phase noise, we propose a novel generalized NS (G-NS) AN precoding design, which mitigates the AN leakage caused to the legitimate user in the presence of phase noise at the expense of a reduction of the available spatial de-

grees of freedom. The proposed method leads to significant performance gains, especially in systems with large numbers of antennas at the BS. Moreover, we generalize the spatially orthogonal (SO) and temporally orthogonal (TO) pilot sequence designs from [22] to orthogonal pilot sequences with arbitrary numbers of non-zero elements. Although SO sequences, which have no zero elements, are preferable for small phase noise variances, sequence designs with zero elements become beneficial in the presence of strong phase noise. Our analytical and numerical results reveal that while hardware impairments in general degrade the achievable secrecy rate, the proposed countermeasures are effective in limiting this degradation. Furthermore, surprisingly, there are cases when the additive distortion noise at the BS is beneficial for the secrecy performance as it can have a similar effect as AN. The work in Chapter 4 was submitted in [65, 66].

1.6 Organization of the Thesis

In the following, we provide a brief overview of the remainder of this thesis. Each of the Chapters 2-4 in this thesis is self-contained and included in separate journal or conference papers. The notations are defined separately for each chapter.

In Chapter 2, we consider physical layer security provisioning in multi-cell massive MIMO systems. Specifically, we consider secure downlink transmission in a multi-cell massive MIMO system with MF precoding and AN precoding at the BS in the presence of a passive multi-antenna eavesdropper. We investigate the resulting achievable ergodic secrecy rate and the secrecy outage probability for the cases of perfect training and pilot contamination. Thereby, we consider two different AN precoding matrices, namely, the conventional AN precoding matrix, where the AN is transmitted in the null space of the matrix formed by all user channels, and a random AN precoding matrix, which avoids the complexity associated with finding the null space of a large matrix.

In Chapter 3, we consider that linear precoding of data and AN are employed for secrecy enhancement. Four different data precoders (i.e., selfish ZF/RCI and collaborative ZF/RCI precoders) and three different AN precoders (i.e., random, selfish/collaborative null-space based precoders) are investigated and the corresponding achievable ergodic secrecy rates are analyzed. Our analysis includes the effects of uplink channel estimation, pilot contamination, multi-cell interference, and path-loss. Furthermore, to strike a balance between complexity and performance, linear precoders that are based on matrix polynomials are proposed for both data and AN precoding. The polynomial coefficients of the data and AN precoders are optimized respectively for minimization of the sum MSE of and the AN leakage to the mobile terminals in the cell of interest using tools from free probability and random matrix theory.

In Chapter 4, we investigate the impact of hardware impairments on the secrecy performance of downlink massive MIMO systems in the presence of a passive multiple-antenna eavesdropper. Thereby, for the BS and the legitimate users, the joint effects of multiplicative phase noise, additive distortion noise, and amplified receiver noise are taken into account, whereas the eavesdropper is assumed to employ ideal hardware. We derive a lower bound for the ergodic secrecy rate of a given user when MF data precoding and AN transmission are employed at the BS. Based on the derived analytical expression, we investigate the impact of the various system parameters on the secrecy rate and optimize both the pilot sets used for uplink training and the AN precoding.

Finally, Chapter 5 summarizes the contributions of this thesis and outlines areas of future research.

Appendices A-C contain the proofs of the propositions, corollaries, lemmas, and theorems used in this thesis.

Chapter 2

AN-Aided MF Precoding in Secure Massive MIMO Systems

2.1 Introduction

Massive MIMO systems offer an abundance of BS antennas, while multiple transmit antennas can be exploited for secrecy enhancement. Therefore, the combination of both concepts seems natural and promising, which is the main motivation for the work presented in this chapter. Several new issues arise for physical layer security provisioning in multi-cell massive MIMO systems that are not present for conventional MIMO systems [10, 23, 27]-[38]. For example, pilot contamination is unique to massive MIMO systems and we study its effect on the ergodic secrecy rate and the secrecy outage probability. Furthermore, for the user data, MF precoding is usually adopted in massive MIMO systems [2, 5], since the matrix inversion needed for the schemes used in conventional MIMO, such as RCI and minimum mean squared error (MMSE) precoding, is considered to be computationally too expensive for the large matrices typical for massive MIMO. Similarly, whereas in conventional MIMO systems, the AN is transmitted in the NS of the channel matrix [24], the complexity associated with computing the NS may not be affordable in case of massive MIMO and simpler AN precoding methods may be needed. Finally, unlike most of the related work [10, 23, 27]-[38], we consider a multi-cell setting where not only the data signals cause inter-cell interference but also the AN, which has to be carefully taken into account for system design.

In this chapter, we study secure downlink transmission in multi-cell massive MIMO systems in the presence of a multi-antenna eavesdropper, which attempts to intercept the signal intended for one of the users. To arrive at an achievable secrecy rate for this user, we assume that the eavesdropper can acquire perfect knowledge of the CSI of all user data channels and is able to cancel all interfering user signals. Under this assumption, we derive tight lower bounds for the ergodic secrecy rate and tight upper bounds for the secrecy outage probability for the cases of perfect training and pilot contamination. The derived bounds are in closed form and provide significant insight for system design. In particular, the obtained results allow us to predict under what conditions (i.e., for what number of BS antennas, eavesdropper antennas, users, path-loss, number of cells, and pilot powers) a positive secrecy rate is possible. Furthermore, we show that employing random AN precoding matrices is an attractive low-complexity option for massive MIMO systems. We also derive a closed-form expression for the fraction of transmit power that should be optimally allocated to AN and show that, for a given number of BS antennas, this fraction increases with the number of eavesdropper antennas and decreases with the number of users in the system.

The remainder of this chapter is organized as follows. In Section 2.2, we describe the channel model, the channel estimation scheme, the transmission format, and two AN precoding matrix designs for the considered system. In Section 2.3, we provide a simple lower bound on the achievable ergodic rate of the MT, a closed-form expression for the ergodic capacity of the eavesdropper, and a simple and tight upper bound for the ergodic capacity of the eavesdropper. In Sections 2.4 and 2.5, we

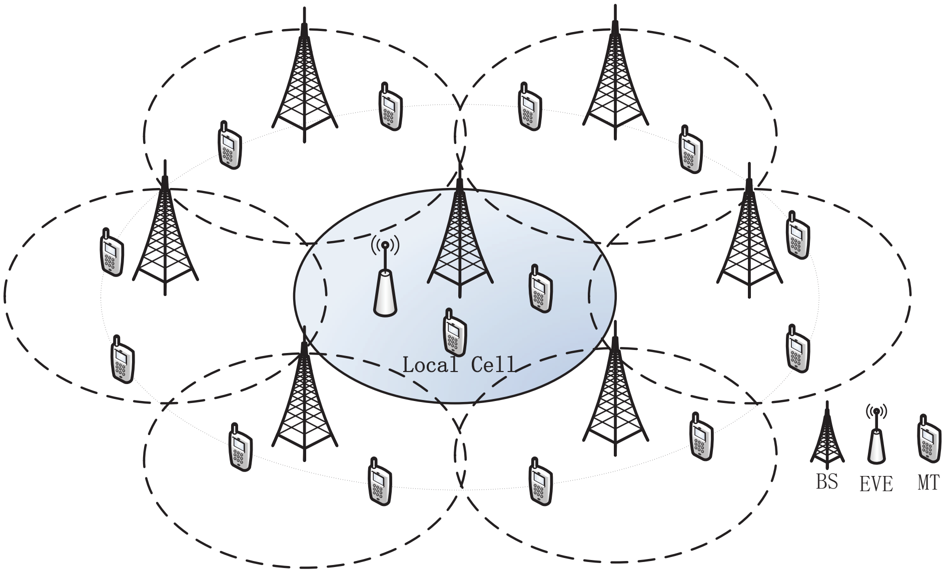

Figure 2.1: Multi-cell massive MIMO system in the presence of a multi-antenna eavesdropper. The shaded cell is the local cell. The MTs in the local cell suffer from the inter-cell interference caused by data and AN transmission in the six adjacent cells.

analyze the secrecy performance of the considered downlink multi-cell massive MIMO system for cases of perfect training and pilot contamination, repsectively. Analytical and simulation results are presented in Section 2.6, and the chapter is concluded in Section 2.7.

2.2 System Model

In this section, we introduce the channel model, the channel estimation scheme, the transmission format, and two AN precoding matrix designs for the considered secure multi-cell massive MIMO system.

2.2.1 System and Channel Models

In this chapter, we consider a flat-fading multi-cell system consisting of M cells, as depicted in Fig. 2.1. Each cell comprises an N_T-antenna BS and K single-antenna MTs [1]. The n^{th} cell, $n \in \{1, \dots, M\}$, is the local cell (the shaded area in Fig. 2.1). An eavesdropper equipped with N_E antennas (equivalent to N_E cooperative single-antenna eavesdroppers) is located in the local cell of the considered multi-cell region. The eavesdropper is passive and seeks to recover the information transmitted to the k^{th} MT in the local cell. Let $\mathbf{g}_{mn}^k \in \mathbb{C}^{1 \times N_T}$ and $\mathbf{G}_{mE} \in \mathbb{C}^{N_E \times N_T}$ denote the channel between the m^{th} BS, $m = 1, \dots, M$, and the k^{th} MT in the local cell and the channel between the m^{th} BS and the eavesdropper, respectively. $\mathbf{g}_{mn}^k = \sqrt{\beta_{mn}^k}\mathbf{h}_{mn}^k$ comprises the path-loss, β_{mn}^k, and the small-scale fading vector, $\mathbf{h}_{mn}^k \sim \mathbb{CN}(\mathbf{0}_{N_T}^T, \mathbf{I}_{N_T})$. Similarly, we model the eavesdropper channel as $\mathbf{G}_{mE} = \sqrt{\beta_{mE}}\mathbf{H}_{mE}$, where β_{mE} and $\mathbf{H}_{mE}$ denote the path-loss and small-scale fading components, respectively. The elements of $\mathbf{H}_{mE}$ are modeled as independent and identically distributed (i.i.d.) Gaussian random variables (r.v.s) with zero mean and unit variance.

2.2.2 Uplink Training and Channel Estimation

We assume that the BSs are perfectly synchronized and operate in the TDD mode with universal frequency reuse. Furthermore, we assume that the path-losses between all users in the system and the local BS, β_{nm}^k, $m = 1, \dots, M$, $k = 1, \dots K$, are known at the local BS, whereas the small-scale fading vectors $\mathbf{h}_{nm}^k$, $m = 1, \dots, M$, $k = 1, \dots K$, are not known and the local BS estimates only the small-scale fading

[1] We note that the results derived in this chapter can be easily extended to multi-antenna MTs if the BS transmits one independent data stream per MT receive antenna and receive combining is not performed at the MTs. In this case, each MT receive antenna can be treated as one (virtual) MT and the results derived in this chapter are applicable. For example, the secrecy rate of a multi-antenna MT can be obtained by summing up the secrecy rates of its receive antennas.

vectors of the MTs within the local cell. These assumptions are motivated by the fact that the path-losses change on a much slower time scale than the small-scale fading vectors, and thus, their estimation creates a comparatively low overhead.

The local BS estimates the downlink CSI of all MTs, $\mathbf{h}_{nn}^{k}$, $k = 1, \ldots, K$, by exploiting reverse training and channel reciprocity [1]-[8]. We consider two scenarios: Perfect training and imperfect training which results in pilot contamination [8]. In the former case, all MK MTs in the system emit orthogonal pilot sequences in the training phase having a sufficiently large pilot power p_τ such that $\hat{\mathbf{h}}_{nn}^{k} = \mathbf{h}_{nn}^{k}$, $k = 1, \ldots, N_T$, can be assumed, where $\hat{\mathbf{h}}_{nn}^{k}$ denotes the estimated channel in the local cell. In the latter case, the K pilot sequences used in a cell are still orthogonal but all cells use the same pilot sequences. Let $\sqrt{\tau}\boldsymbol{\omega}_k \in \mathbb{C}^{\tau \times 1}$ denote the pilot sequence of length τ transmitted by the k^{th} MT in each cell in the training phase, where $\boldsymbol{\omega}_k^H \boldsymbol{\omega}_k = 1$ and $\boldsymbol{\omega}_k^H \boldsymbol{\omega}_j = 0$, $\forall, j, k = 1, \ldots, K$, $k \neq j$. Assuming perfect synchronization, the training signal received at the local BS, $\mathbf{Y}_n^{\text{pilot}} \in \mathbb{C}^{\tau \times N_T}$, can be expressed as

$$\mathbf{Y}_n^{\text{pilot}} = \sum_{m=1}^{M} \sum_{k=1}^{K} \sqrt{p_\tau \tau \beta_{nm}^{k}} \boldsymbol{\omega}_k \mathbf{h}_{nm}^{k} + \mathbf{N}_n, \tag{2.1}$$

where $\mathbf{N}_n \in \mathbb{C}^{\tau \times N_T}$ is a Gaussian noise matrix having zero mean, unit variance elements. Assuming MMSE channel estimation [7, 8], the estimate of $\mathbf{h}_{nn}^{k}$ given $\mathbf{Y}_n^{\text{pilot}}$ is obtained as

$$\begin{aligned} \hat{\mathbf{h}}_{nn}^{k} &= \sqrt{p_\tau \tau \beta_{nn}^{k}} \boldsymbol{\omega}_k^H \left(\mathbf{I}_\tau + \boldsymbol{\omega}_k \left(p_\tau \tau \sum_{m=1}^{M} \beta_{nm}^{k} \right) \boldsymbol{\omega}_k^H \right)^{-1} \mathbf{Y}_n^{\text{pilot}} \\ &= \frac{\sqrt{p_\tau \tau \beta_{nn}^{k}}}{1 + p_\tau \tau \sum_{m=1}^{M} \beta_{nm}^{k}} \boldsymbol{\omega}_k^H \mathbf{Y}_n^{\text{pilot}}. \end{aligned} \tag{2.2}$$

For MMSE estimation, we can express the channel as $\mathbf{h}_{nn}^{k} = \hat{\mathbf{h}}_{nn}^{k} + \tilde{\mathbf{h}}_{nn}^{k}$, where the estimate $\hat{\mathbf{h}}_{nn}^{k}$ and the estimation error $\tilde{\mathbf{h}}_{nn}^{k} \in \mathbb{C}^{1\times N_T}$ are mutually independent. Hence, considering (2.2) we can statistically characterize $\hat{\mathbf{h}}_{nn}^{k}$ and $\tilde{\mathbf{h}}_{nn}^{k}$ as $\hat{\mathbf{h}}_{nn}^{k} \sim \mathbb{CN}\left(\mathbf{0}_{N_T}^{T}, \frac{p_\tau \tau \beta_{nn}^{k}}{1+p_\tau \tau \sum_{m=1}^{M}\beta_{nm}^{k}}\mathbf{I}_{N_T}\right)$ and $\tilde{\mathbf{h}}_{nn}^{k} \sim \mathbb{CN}\left(\mathbf{0}_{N_T}^{T}, \frac{1+p_\tau \tau \sum_{m\neq n}\beta_{nm}^{k}}{1+p_\tau \tau \sum_{m=1}^{M}\beta_{nm}^{k}}\mathbf{I}_{N_T}\right)$, respectively. Still from (2.2), we also observe that $\boldsymbol{\omega}_k^H \mathbf{Y}_n^{\text{pilot}}$ is proportional to the MMSE estimate of $\mathbf{h}_{nm}^{k}$ for any m, i.e.,

$$\frac{\hat{\mathbf{h}}_{nm}^{k}}{\|\hat{\mathbf{h}}_{nm}^{k}\|} = \frac{\boldsymbol{\omega}_k^H \mathbf{Y}_n^{\text{pilot}}}{\|\boldsymbol{\omega}_k^H \mathbf{Y}_n^{\text{pilot}}\|}, \forall m. \tag{2.3}$$

Eq. (2.3) implies that the estimate of the k^{th} MT in each cell is simply a scaled version of the same vector $\boldsymbol{\omega}_k^H \mathbf{Y}_n^{\text{pilot}}$. Hence, the BS is not able to distinguish between the channel to its k^{th} MT and to the k^{th} MT in other cells [8]. In the same manner, we also expand the channel $\mathbf{h}_{mn}^{k} = \hat{\mathbf{h}}_{mn}^{k} + \tilde{\mathbf{h}}_{mn}^{k}$, [2] where $\hat{\mathbf{h}}_{mn}^{k}$ and $\tilde{\mathbf{h}}_{mn}^{k}$ are mutually independent. We also have $\hat{\mathbf{h}}_{mn}^{k} \sim \mathbb{CN}\left(\mathbf{0}_{N_T}^{T}, \frac{p_\tau \tau \beta_{mn}^{k}}{1+p_\tau \tau \sum_{l=1}^{M}\beta_{ml}^{k}}\mathbf{I}_{N_T}\right)$ and $\tilde{\mathbf{h}}_{mn}^{k} \sim \mathbb{CN}\left(\mathbf{0}_{N_T}^{T}, \frac{1+p_\tau \tau \sum_{l\neq n}\beta_{ml}^{k}}{1+p_\tau \tau \sum_{l=1}^{M}\beta_{ml}^{k}}\mathbf{I}_{N_T}\right)$, respectively.

In order to be able to find the required numbers of orthogonal pilot sequences, pilot sequence lengths of $\tau \geq MK$ and $\tau \geq K$ are required for the cases of perfect training and pilot contamination, respectively. Furthermore, we note that the eavesdropper could emit his own pilot symbols to impair the channel estimates obtained at the BS to improve his ability to decode the MTs' signals during downlink transmission [44]. However, this would also increase the chance that the presence of the eavesdropper is detected by the BS [45]. Therefore, in this chapter, we assume the eavesdropper is purely passive and leave the study of active eavesdroppers in massive MIMO systems for future work.

[2] In this chapter, the local BS only needs to estimate $\mathbf{h}_{nn}^{k}$. The role of this expansion is to facilitate a mathematical simplification in deriving the achievable rate in Section 2.5 for the case of pilot contamination, by decomposing the inter-cell interference/AN leakage from the m^{th} cell into correlated terms $\hat{\mathbf{h}}_{mn}^{k}$ and uncorrelated terms $\tilde{\mathbf{h}}_{mn}^{k}$ with respect to (w.r.t.) the desired MT's channel estimate.

2.2.3 Downlink Data Transmission

In the local cell, the BS intends to transmit a confidential signal s_{nk} to the k^{th} MT. The signal vector for the K MTs is denoted by $\mathbf{s}_n = \left[s_{n1}, \ldots, s_{nK}\right]^T \in \mathbb{C}^{K\times 1}$ with $\mathbb{E}[\mathbf{s}_n\mathbf{s}_n^H] = \mathbf{I}_K$. Each signal vector $\mathbf{s}_n$ is multiplied by a transmit beamforming matrix, $\mathbf{F}_n = [\mathbf{f}_{n1}, \ldots, \mathbf{f}_{nk}, \ldots, \mathbf{f}_{nK}] \in \mathbb{C}^{N_T\times K}$, before transmission. As typical for massive MIMO systems, we adopt simple MF precoding, i.e., $\mathbf{f}_{nk} = (\hat{\mathbf{h}}_{nn}^k)^H/\|\hat{\mathbf{h}}_{nn}^k\|$ [5],[8], since the matrix inversion required for ZF and MMSE precoding is computationally too expensive for the large number of users and antenna elements that are typical for massive MIMO systems. Furthermore, we assume that the eavesdropper's CSI is not available at the local BS. Hence, assuming that there are $K < N_T$ MTs, the BS may use the remaining $N_T - K$ degrees of freedom offered by the N_T transmit antennas for emission of AN to degrade the eavesdropper's ability to decode the data intended for the MTs [24, 37, 38]. The AN vector, $\mathbf{z}_n = [z_{n1}, \ldots, z_{n(N_T-K)}]^T \sim \mathbb{CN}(\mathbf{0}_{N_T-K}, \mathbf{I}_{N_T-K})$, is multiplied by an AN precoding matrix $\mathbf{A}_n = [\mathbf{a}_{n1}, \ldots, \mathbf{a}_{ni}, \ldots, \mathbf{a}_{n(N_T-K)}] \in \mathbb{C}^{N_T\times(N_T-K)}$ with $\|\mathbf{a}_{ni}\| = 1$, $i = 1, \ldots, N_T - K$. The considered choices for the AN precoding matrix will be discussed in the next subsection. The signal vector transmitted by the local BS is given by

$$\mathbf{x}_n = \sqrt{p}\mathbf{F}_n\mathbf{s}_n + \sqrt{q}\mathbf{A}_n\mathbf{z}_n = \sum_{k=1}^{K}\sqrt{p}\mathbf{f}_{nk}s_{nk} + \sum_{i=1}^{N_T-K}\sqrt{q}\mathbf{a}_{ni}z_{ni}, \tag{2.4}$$

where p and q denote the transmit power allocated to each MT and each AN signal, respectively, i.e., for simplicity, we assume uniform power allocation across users and AN signals, respectively. Let the total transmit power be denoted by P_T. Then, p and q can be represented as $p = \frac{\phi P_T}{K}$ and $q = \frac{(1-\phi)P_T}{N_T-K}$, respectively, where the power allocation factor ϕ, $0 < \phi \leq 1$, strikes a power balance between the information-bearing signal and the AN.

The $M-1$ cells adjacent to the local cell transmit their own signals and AN. In this work, in order to be able to gain some fundamental insights, we assume that all cells employ identical values for p and q as well as ϕ. Accordingly, the received signals at the k^{th} MT in the local cell, y_{nk}, and at the eavesdropper, $\mathbf{y}_E$, are given by

$$y_{nk} = \sqrt{p}\mathbf{h}_{nn}^{k}\mathbf{f}_{nk}s_{nk} + \sum_{\{m,l\}\neq\{n,k\}} \sqrt{p}\mathbf{h}_{mn}^{k}\mathbf{f}_{ml}s_{ml} + \sum_{m=1}^{M} \sqrt{q}\mathbf{h}_{mn}^{k}\mathbf{A}_m\mathbf{z}_m + n_{nk} \tag{2.5}$$

and

$$\mathbf{y}_E = \sqrt{p}\sum_{m=1}^{M} \mathbf{H}_{mE}\mathbf{F}_m\mathbf{s}_m + \sqrt{q}\sum_{m=1}^{M} \mathbf{H}_{mE}\mathbf{A}_m\mathbf{z}_m + \mathbf{n}_E, \tag{2.6}$$

respectively, where $n_{nk} \sim \mathbb{CN}(0, \sigma_{nk}^2)$ and $\mathbf{n}_E \sim \mathbb{CN}(\mathbf{0}_{N_E}, \sigma_E^2\mathbf{I}_{N_E})$ are the Gaussian noises at the k^{th} MT and at the eavesdropper, respectively. The first term on the right hand side of (2.5) is the signal intended for the k^{th} MT in the local cell with effective channel gain $\sqrt{p}\mathbf{h}_{nn}^{k}\mathbf{f}_{nk}$, which is assumed to be perfectly known at the k^{th} MT in the local cell. The second and the third terms on the right hand side of (2.5) represent intra-cell/inter-cell interference and AN leakage, respectively. On the other hand, the eavesdropper observes an $MN_T \times N_E$ MIMO channel comprising K local user signals, $(M-1)K$ out-of-cell user signals, $N_T - K$ local cell AN signals, and $(N_T - K)(M-1)$ out-of-cell AN signals. In order to obtain a lower bound on the achievable secrecy rate, we assume that the eavesdropper can acquire perfect knowledge of the effective channels of all MTs, i.e., $\mathbf{H}_{mE}\mathbf{f}_{mk}, \forall m, k$. We note however that this is a quite pessimistic assumption because the uplink training performed in massive MIMO [8] makes it difficult for the eavesdropper to perform accurate channel estimation.

2.2.4 Design of AN Precoding Matrix $\mathbf{A}_n$

In this chapter, we consider two different designs for the AN precoding matrix $\mathbf{A}_n$.

NS method: For conventional (non-massive) MIMO, $\mathbf{A}_n$ is usually chosen to lie in the null space of the estimated channel, $\hat{\mathbf{h}}_{nn}^k$, i.e., $\hat{\mathbf{h}}_{nn}^k \mathbf{A}_n = \mathbf{0}_{N_T-K}^T$, $k = 1, \ldots, K$, which is possible as long as $N_T > K$ holds [24]. We refer to this method as $\mathcal{N}$ in the following. If perfect CSI is available, i.e., $\hat{\mathbf{h}}_{nn}^k = \mathbf{h}_{nn}^k$, the $\mathcal{N}$-method prevents impairment of the users in the local cell by AN generated by the local BS. In case of pilot contamination, intra-cell AN leakage to the users in the local cell is unavoidable, but inter-cell AN leakage is suppressed due to pilot contamination, which is an extra benefit, and will be discussed in Section 2.5 in details. Unfortunately, for the large values of N_T and K typical for massive MIMO systems, computation of the NS of $\hat{\mathbf{h}}_{nn}^k$, $k = 1, \ldots, K$, is computationally expensive. This motivates the introduction of a simpler method for generation of the AN precoding matrix.

Random method: In this case, the columns of $\mathbf{A}_n$ are mutually independent random vectors. We refer to this method as $\mathcal{R}$ in the following. Here, we construct the columns of $\mathbf{A}_n$ as $\mathbf{a}_{ni} = \tilde{\mathbf{a}}_{ni}/\|\tilde{\mathbf{a}}_{ni}\|$, where the $\tilde{\mathbf{a}}_{ni}$, $i = 1, \ldots, N_T - K$, are mutually independent Gaussian random vectors. Note that the $\mathcal{R}$-method does not even attempt to avoid AN leakage to the users in the local cell. However, it may still improve the ergodic secrecy rate as the precoding vector for the desired user signal, $\mathbf{f}_{nk}$, is correlated with the user channel, $\mathbf{h}_{nn}^k$, whereas the columns of the AN precoding matrix are not correlated with the user channel.

Our results in Sections 2.4-2.6 reveal that although the $\mathcal{N}$-method always achieves a better performance than the $\mathcal{R}$-method, if pilot contamination and inter-cell interference are significant, the performance differences between both schemes are small. This makes the $\mathcal{R}$-method an attractive alternative for massive MIMO systems due to its simplicity.

2.3 Achievable Ergodic Secrecy Rate Analysis

In this section, we first show that the achievable ergodic secrecy rate of the k^{th} MT in the local cell can be expressed as the difference between the achievable ergodic rate of the MT and the ergodic capacity of the eavesdropper. Subsequently, we provide a simple lower bound on the achievable ergodic rate of the MT, a closed-form expression for the ergodic capacity of the eavesdropper, and a simple and tight upper bound for the ergodic capacity of the eavesdropper. The results derived in this section are valid for both perfect training and pilot contamination as well as for both AN precoding matrix designs. For convenience, we define the ratio of the number of eavesdropper antennas and the number of BS antennas as $\alpha = N_E/N_T$, and the ratio of the number of users and the number of BS antennas as $\beta = K/N_T$. In the following, we are interested in the asymptotic regime where $N_T \to \infty$ but α and β are constant.

2.3.1 Achievable Ergodic Secrecy Rate

The ergodic secrecy rate is an appropriate performance measure if delays can be afforded and coding over many independent channel realizations (i.e., over many coherence intervals) is possible [25]. Considering the k^{th} MT in the local cell, the considered channel is an instance of a multiple-input, single-output, multiple eavesdropper (MISOME) wiretap channel [27]. In the following lemma, we provide an expression for an achievable ergodic secrecy rate of the k^{th} MT in the local cell.

Lemma 2.1. *An achievable ergodic secrecy rate of the k^{th} MT in the local cell is* *given by*

$$R_{nk}^{\mathrm{sec}} = [R_{nk} - C_{nk}^{\mathrm{eve}}]^{+}, \tag{2.7}$$

where $[x]^{+} = \max\{0, x\}$*,* R_{nk} *is an achievable ergodic rate of the* k^{th} *MT in the local cell, and* C_{nk}^{eve} *is the ergodic capacity between the local BS and the eavesdropper seeking to decode the information of the* k^{th} *MT in the local cell. Thereby, it is assumed that the eavesdropper is able to cancel the received signals of all in-cell and out-of-cell MTs except the signal intended for the MT of interest, i.e.,*

$$C_{nk}^{\mathrm{eve}} = \mathbb{E}\left[\log_2\left(1 + p\mathbf{f}_{nk}^{H}\mathbf{G}_{nE}^{H}\mathbf{X}^{-1}\mathbf{G}_{nE}\mathbf{f}_{nk}\right)\right], \tag{2.8}$$

where $\mathbf{X} = q\sum_{m=1}^{M}\mathbf{A}_{m}^{H}\mathbf{G}_{mE}^{H}\mathbf{G}_{mE}\mathbf{A}_{m}$ *denotes the noise correlation matrix at the eavesdropper under the worst-case assumption that the receiver noise is negligible, i.e.,* $\sigma_E^2 \to 0$.

Proof. Please refer to Appendix A.1. □

Eq. (2.7) reveals that the achievable ergodic secrecy rate of the k^{th} MT in the local cell has the subtractive form typical for many wiretap channels [10, 23, 27]-[38], i.e., it is the difference of an achievable ergodic rate of the user of interest and the capacity of the eavesdropper. Before we analyze (2.7) for perfect training and pilot contamination in Sections 2.4 and 2.5, respectively, we derive general expressions for R_{nk} and C_{nk}^{eve}, which apply to both cases.

2.3.2 Lower Bound on the Achievable User Rate

Based on (2.5) an achievable ergodic rate of the k^{th} MT in the local cell is given by $R_{nk} =$

$$\mathbb{E}\left[\log_2\left(1+\frac{|\sqrt{p}\mathbf{g}_{nn}^{k}\mathbf{f}_{nk}|^2}{\sum_{m=1}^{M}\sum_{i=1}^{N_T-K}|\sqrt{q}\mathbf{g}_{mn}^{k}\mathbf{a}_{mi}|^2+\sum_{\{m,l\}\neq\{n,k\}}|\sqrt{p}\mathbf{g}_{mn}^{k}\mathbf{f}_{ml}|^2+\sigma_{nk}^2}\right)\right]. \tag{2.9}$$

Unfortunately, evaluating the expected value in (2.9) analytically is cumbersome. Therefore, we derive a lower bound on the achievable ergodic rate of the k^{th} MT in the local cell by following the same approach as in [8]. In particular, we rewrite the received signal at the k^{th} MT in the local cell as

$$y_{nk} = \mathbb{E}[\sqrt{p}\mathbf{g}_{nn}^{k}\mathbf{f}_{nk}]s_{nk} + n'_{nk}, \tag{2.10}$$

where n'_{nk} represents an effective noise, which is given by $n'_{nk} =$

$$\left(\sqrt{p}\mathbf{g}_{nn}^{k}\mathbf{f}_{nk} - \mathbb{E}[\sqrt{p}\mathbf{g}_{nn}^{k}\mathbf{f}_{nk}]\right)s_{nk} + \sum_{m=1}^{M}\mathbf{g}_{mn}^{k}\sqrt{q}\mathbf{A}_m\mathbf{z}_m + \sum_{\{m,l\}\neq\{n,k\}}\sqrt{p}\mathbf{g}_{mn}^{k}\mathbf{f}_{ml}s_{ml} + n_{nk}. \tag{2.11}$$

Eq. (2.10) can be interpreted as an equivalent single-input single-output channel with constant gain $\mathbb{E}[\sqrt{p}\mathbf{g}_{nn}^{k}\mathbf{f}_{nk}]$ and AWGN n'_{nk}. Hence, we can apply Theorem 1 in [8] to obtain a computable lower bound for the achievable rate of the k^{th} MT in the local cell as $\underline{R}_{nk} = \log_2(1+\gamma_{nk}) \leq R_{nk}$, where γ_{nk} denotes the received signal-to-interference-plus-noise ratio (SINR), given by $\gamma_{nk} =$

$$\frac{\overbrace{|\mathbb{E}[\sqrt{p}\mathbf{g}_{nn}^{k}\mathbf{f}_{nk}]|^2}^{\text{desired signal}}}{\underbrace{\text{var}[\sqrt{p}\mathbf{g}_{nn}^{k}\mathbf{f}_{nk}]}_{\text{signal leakage}} + \underbrace{\sum_{m=1}^{M}\sum_{i=1}^{N_T-K}\mathbb{E}[|\sqrt{q}\mathbf{g}_{mn}^{k}\mathbf{a}_{mi}|^2] }_{\text{AN leakage}}+ \underbrace{\sum_{\{m,l\}\neq\{n,k\}}\mathbb{E}[|\sqrt{p}\mathbf{g}_{mn}^{k}\mathbf{f}_{ml}|^2]}_{\text{intra- and inter-cell interference}} + \sigma_{nk}^2} \tag{2.12}$$

with $\text{var}[\sqrt{p}\mathbf{g}_{nn}^{k}\mathbf{f}_{nk}] = \mathbb{E}[|\sqrt{p}\mathbf{g}_{nn}^{k}\mathbf{f}_{nk} - \mathbb{E}[\sqrt{p}\mathbf{g}_{nn}^{k}\mathbf{f}_{nk}]|^2]$. We note that the derived lower bound on the achievable rate is applicable to both AN precoding matrix designs and the cases of perfect training and pilot contamination, respectively, cf. Sections 2.4 and 2.5. The tightness of the lower bound will be confirmed by our results in Section 2.6.

2.3.3 Ergodic Capacity of the Eavesdropper

In this section, we provide a closed-form expression for the ergodic capacity of the eavesdropper valid for both perfect training and pilot contamination. To gain more insight, we adopt a simplified path-loss model for the eavesdropper, i.e., the path-losses between the BSs and the eavesdropper are given by $\beta_{mE} = 1$ if $n = m$ and $\beta_{mE} = \rho$ if $n \neq m$, i.e., the path-loss between the local BS and the eavesdropper is 1 and the path-loss between the BSs of the other cells and the eavesdropper is $\rho \in [0, 1]$.[3] A similar simplified path-loss model was used in [7] for the user channels. The resulting ergodic secrecy capacity is summarized in the following theorem.

Theorem 2.1. *For $N_T \to \infty$ and both the $\mathcal{N}$ and the $\mathcal{R}$ AN precoding matrix designs,*

[3] We note that the simplified path-loss model is only adopted to reduce the number of parameters. The ergodic capacity and the ergodic secrecy rate can also be derived for the original path-loss model in closed form. However, the resulting equations are more cumbersome and less insightful compared to those for the simplified model.

the ergodic capacity of the eavesdropper in (2.8) can be written as

$$C_{nk}^{\text{eve}} = \frac{1}{\ln 2} \sum_{i=0}^{N_E-1} \lambda_i \times \frac{1}{\mu_0} \sum_{j=1}^{2} \sum_{l=2}^{b_j} \omega_{jl} I(1/\mu_j, l), \tag{2.13}$$

where $\lambda_i = \binom{M(N_T-K)}{i}$, $\mu_0 = \prod_{j=1}^{2} \mu_j^{b_j}$,

$$(\mu_j, b_j) = \begin{cases} (\eta, N_T - K), & j = 1 \\ (\rho\eta, (M-1)(N_T - K)), & j = 2, \end{cases} \tag{2.14}$$

$\eta = q/p$,

$$\omega_{jl} = \frac{1}{(b_j - l)!} \frac{d^{b_j - l}}{dx^{b_j - l}} \left(\frac{x^i}{\prod_{s \neq j} (x + \frac{1}{\mu_s})^{b_s}} \right) \Bigg|_{x = -\frac{1}{\mu_j}}, \tag{2.15}$$

and $I(a,n) = \int_0^\infty \frac{1}{(x+1)(x+a)^n} dx, \; a, n > 0$. *A closed-form expression for* $I(\cdot,\cdot)$ *is given in [67, Lemma 3].*

Proof. Please refer to Appendix A.2. □

A lower bound on the achievable ergodic secrecy rate of the k^{th} MT in the local cell for the $\mathcal{N}/\mathcal{R}$ methods is obtained by combining (2.7), (2.12), and (2.13). However, the expression for the ergodic capacity of the eavesdropper in (2.13) is somewhat cumbersome and offers little insight into the impact of the various system parameters. Hence, in the next subsection, we derive a simple and tight upper bound for C_{nk}^{eve}.

2.3.4 Tight Upper Bound on the Ergodic Capacity of the Eavesdropper

In the following theorem, we provide a tight upper bound for the ergodic capacity of the eavesdropper.

Theorem 2.2. *For $N_T \to \infty$ and both the $\mathcal{N}$ and the $\mathcal{R}$ AN precoding matrix generation methods, the ergodic capacity of the eavesdropper in (2.8) is upper bounded by* [4]

$$C_{nk}^{\mathrm{eve}} < \overline{C}_{nk}^{\mathrm{eve}} \approx \log_2\left(1 + \frac{\alpha}{\eta a(1-\beta) - c\eta\alpha/a}\right) = \log_2\left(\frac{(1-\zeta)\phi + \zeta}{-\zeta\phi + \zeta}\right), \qquad (2.16)$$

if $\beta < 1 - c\alpha/a^2$, where we introduce the definitions $a = 1+\rho(M-1)$, $c = 1+\rho^2(M-1)$, and $\zeta = \frac{a\beta}{\alpha} - \frac{\beta c}{a(1-\beta)}$.

Proof. Please refer to Appendix A.3. □

Remark 2.1. *We note that a finite eavesdropper capacity results only if matrix $\mathbf{X}$ in (2.8) is invertible. Since $\mathbf{G}_{mE}$, $m = 1, \ldots, M$, are independent matrices with i.i.d. entries, $\mathbf{X}$ is invertible if $M(N_T - K) \leq N_E$ or equivalently $\beta \leq 1 - \alpha/M$. Regardless of the values of M and ρ, we have*

$$1 - \alpha/[1 + \rho^2(M-1)] \leq 1 - c\alpha/a^2 \leq 1 - \alpha/M. \qquad (2.17)$$

For $M = 1$ or $\rho = 1$, equality holds in (2.17). For $M > 1$ and $\rho < 1$, the condition for β in Theorem 2.2 is in general stricter than the invertibility condition for $\mathbf{X}$. Nevertheless, the typical operating region for a massive MIMO system is $\beta \ll 1$ [2, 5], where the upper bound in Theorem 2.2 is applicable.

Eq. (2.16) reveals that $\overline{C}_{nk}^{\mathrm{eve}}$ is monotonically increasing in α, i.e., as expected, the eavesdropper can enhance his eavesdropping capability by deploying more antennas. Furthermore, in the relevant parameter range, $0 < \beta < 1 - c\alpha/a^2$, $\overline{C}_{nk}^{\mathrm{eve}}$ is not

[4] We note that, strictly speaking, we have not proved that (2.16) is a bound since we used an approximation for its derivation, see Appendix C. However, this approximation is known to be very accurate [69] and comparisons of (2.16) with simulation results for various system parameters suggest that (2.16) is indeed an upper bound.

monotonic in β but a decreasing function for $\beta \in (0, 1 - \sqrt{c\alpha}/a)$ and an increasing function for $\beta \in (1 - \sqrt{c\alpha}/a, 1 - c\alpha/a^2)$. Hence, $\overline{C}_{nk}^{\mathrm{eve}}$ has a minimum at $\beta = 1 - \sqrt{c\alpha}/a$. Assuming N_T and N_E are fixed, this behaviour can be explained as follows. For small K (corresponding to small β), the capacity of the eavesdropper is large because the amount of power allocated to the intercepted MT, $\phi P_T/K$, is large. As K increases, the power allocated to the MT decreases which leads to a decrease in the capacity. However, if K is increased beyond a certain point, $\mathbf{X}$ becomes increasingly ill-conditioned which leads to an increase in the eavesdropper capacity.

Combining now (2.7), (2.12), and (2.16) gives a tight lower bound on the ergodic secrecy rate of the k^{th} MT in the local cell for both the $\mathcal{N}$ and the $\mathcal{R}$ methods. To gain more insight, in the next two sections, we specialize the tight lower bound on the ergodic secrecy rate to the cases of perfect training and pilot contamination, respectively. This will allow us to further simplify the SINR expression of the k^{th} MT in the local cell and the resulting ergodic secrecy rate expression.

2.4 Performance Analysis for Perfect Training

In this section, we analyze the secrecy performance of the considered downlink multi-cell massive MIMO system under the assumption of perfect CSI, i.e., $\hat{\mathbf{h}}_{nn}^k = \mathbf{h}_{nn}^k$, $k = 1, \ldots, K$. To this end, for both considered AN precoding methods, we first simplify the lower bound on the achievable ergodic rate expression derived in Section 2.3.2 by taking into account the perfect CSI assumption. Subsequently, exploiting this result, we derive simple and insightful lower bounds on the achievable ergodic secrecy rate. Finally, we obtain an upper bound on the secrecy outage probability.

2.4.1 Lower Bound on the Achievable Ergodic Rate

We first characterize some of the terms in (2.12) for the case of perfect training in the following lemma.

Lemma 2.2. *The received signal and interference powers at the k^{th} MT in the local cell can be expressed as*

$$\mathbb{E}[\mathbf{h}_{nn}^k \mathbf{f}_{nk}]^2 = \mathbb{E}^2[x] \quad \text{and} \quad \mathbb{E}[|\mathbf{h}_{nn}^k \mathbf{f}_{mk}|^2] = \mathbb{E}[|\mathbf{h}_{nn}^k \mathbf{a}_{mi}|^2] = \mathbb{E}[y^2], \forall n \neq m \tag{2.18}$$

respectively, where $x^2 = \sum_{l=1}^{N_T} |u_l|^2 \sim \chi^2_{2N_T}$, $y^2 = |u_l|^2 \sim \chi^2_2$, u_l are i.i.d. complex Gaussian r.v.s with zero mean and unit variance, and $\mathbb{E}[y^2] = 1$.

Proof. Since each element of $\mathbf{h}_{nn}^k$ follows a Gaussian distribution with zero mean and unit variance and $\mathbf{f}_{nk} = \frac{(\mathbf{h}_{nn}^k)^H}{\|\mathbf{h}_{nn}^k\|} = \frac{(\mathbf{h}_{nn}^k)^H}{\|\mathbf{h}_{nn}^k\|}$, $|\mathbf{h}_{nn}^k \mathbf{f}_{nk}|^2$ is a (scaled) chi-square r.v. with $2N_T$ degrees of freedom and statistically equivalent to x^2. On the other hand, since $\mathbf{f}_{ml}$, $\forall\{m,l\} \neq \{n,k\}$, and $\mathbf{a}_{mi}$ are unit-norm vectors and independent of the small-scale fading vector $\mathbf{h}_{nn}^k$, the normalized interference terms, $|\mathbf{h}_{nn}^k \mathbf{f}_{mk}|^2$ and $|\mathbf{h}_{nn}^k \mathbf{a}_{mi}|^2$, are (scaled) chi-square r.v.s with 2 degrees of freedom and statistically equivalent to y^2. □

Introducing x and y in (2.12) and dividing both numerator and denominator by p, we obtain the SINRs for the $\mathcal{N}$ and $\mathcal{R}$ AN precoding matrices as

$$\gamma_{nk}^{\mathcal{N}} = \frac{\beta_{nn}^k \mathbb{E}^2[x]}{\beta_{nn}^k \text{var}[x] + \eta \sum_{m\neq n}^{M} \beta_{mn}^k \sum_{i=1}^{N_T-K} \mathbb{E}[y^2] + \sum_{\{m,l\}\neq\{n,k\}} \beta_{mn}^k \mathbb{E}[y^2] + \frac{K}{\phi P_T}} \tag{2.19}$$

and

$$\gamma_{nk}^{\mathcal{R}} = \frac{\beta_{nn}^k \mathbb{E}^2[x]}{\beta_{nn}^k \text{var}[x] + \eta \sum_{m=1}^{M} \beta_{mn}^k \sum_{i=1}^{N_T-K} \mathbb{E}[y^2] + \sum_{\{m,l\}\neq\{n,k\}} \beta_{mn}^k \mathbb{E}[y^2] + \frac{K}{\phi P_T}}, \tag{2.20}$$

respectively. The right hand sides of (2.19) and (2.20) differ only in the second term of the denominator, where $\gamma_{nk}^{\mathcal{R}}$ contains an additional term $\eta\beta_{nn}^{k}\sum_{i=1}^{N_T-K}\mathbb{E}[y^2]$, which is due to the AN leakage caused in the local cell. This term is absent in $\gamma_{nk}^{\mathcal{N}}$ as, for perfect CSI, the $\mathcal{N}$-method avoids AN leakage in the local cell. Hence, $\gamma_{nk}^{\mathcal{N}} > \gamma_{nk}^{\mathcal{R}}$ always holds. Since for large N_T we have [8]

$$\lim_{N_T\to\infty}\frac{\mathbb{E}^2[x]}{N_T} = 1 \text{ and } \lim_{N_T\to\infty}\frac{\mathrm{var}[x]}{N_T} = 0, \tag{2.21}$$

we obtain from (2.19) and (2.20)

$$\lim_{N_T\to\infty}\gamma_{nk}^{\mathcal{N}} = \frac{\beta_{nn}^{k}N_T}{\eta\sum_{m\neq n}^{M}\beta_{mn}^{k}(N_T-K)+\sum_{\{m,l\}\neq\{n,k\}}\beta_{mn}^{k}+\frac{K}{\phi P_T}} \tag{2.22}$$

and

$$\lim_{N_T\to\infty}\gamma_{nk}^{\mathcal{R}} = \frac{\beta_{nn}^{k}N_T}{\eta\sum_{m=1}^{M}\beta_{mn}^{k}(N_T-K)+\sum_{\{m,l\}\neq\{n,k\}}\beta_{mn}^{k}+\frac{K}{\phi P_T}}, \tag{2.23}$$

respectively. In order to obtain simple yet insightful results, we adopt in the following a simplified path-loss model [7], similar to the simplified model introduced for the eavesdropper in Section 2.3.3. In particular, we model the path-losses as $\beta_{mn}^{k} = 1$ if $n = m$ and $\beta_{mn}^{k} = \rho$ if $n \neq m$, i.e., the path-loss between the local BS and the MTs in the local cell is 1 and the path-loss between the BSs of the other cells and the MTs in the local cell is ρ. Hence, (2.22) and (2.23) simplify to

$$\lim_{N_T\to\infty}\gamma_{nk}^{\mathcal{N}} = \frac{1}{(M-1)\rho(1-\beta)\eta+(M-1)\beta\rho+\beta+\frac{\beta}{\phi P_T}} \tag{2.24}$$

and

$$\lim_{N_T\to\infty}\gamma_{nk}^{\mathcal{R}} = \frac{1}{((M-1)\rho+1)(1-\beta)\eta+(M-1)\beta\rho+\beta+\frac{\beta}{\phi P_T}}, \tag{2.25}$$

respectively. The ergodic rate for the two considered AN precoding matrix generation methods is lower bounded by $\underline{R}_{nk}^{\Psi} = \log_2(1+\gamma_{nk}^{\Psi})$, where $\Psi \in \{\mathcal{N}, \mathcal{R}\}$. We note that for systems with few users, i.e., $\beta \to 0$, and $N_T \to \infty$, the lower bounds on the ergodic rate reduce to

$$\underline{R}_{nk}^{\mathcal{N}} \approx \log_2\left(1+\frac{1}{\eta(M-1)\rho}\right) \quad \text{and} \quad \underline{R}_{nk}^{\mathcal{R}} \approx \log_2\left(1+\frac{1}{\eta((M-1)\rho+1)}\right), \tag{2.26}$$

i.e., performance is limited by AN leakage. This is in contrast to massive MIMO systems without AN precoding, whose performance in the considered regime ($\beta \to 0$) is only limited by pilot contamination [2, 5], which is not considered in this section but will be addressed in Section V. Moreover, (2.26) suggests that the performance difference between the $\mathcal{N}$-method and the $\mathcal{R}$-method diminishes if the AN leakage from adjacent cells, which is proportional to $\eta(M-1)\rho$ for both methods, dominates the AN leakage for the $\mathcal{R}$-method in the local cell, which is proportional to η.

Closed-form expressions for the lower bound on the achievable ergodic secrecy rate of the k^{th} MT in the local cell for the $\mathcal{N}/\mathcal{R}$ methods are obtained by combining (2.7), (2.13), and (2.24)/(2.25). The tightness of the proposed lower bounds will be confirmed in Section 2.6 via simulations.

2.4.2 Impact of System Parameters on Ergodic Secrecy Rate

In this subsection, we provide insight into the influence of the various system parameters on the ergodic secrecy rate. Combining (2.7), (2.24)/(2.25), and the upper bound on the ergodic secrecy capacity in (2.16), simple lower bounds for the ergodic secrecy rate valid for $N_T \to \infty$ are obtained as

$$\underline{R}_{nk}^{\text{sec},\mathcal{N}} = \left[\log_2\left(\frac{b\beta\zeta + (\beta+1-b\beta)\zeta\phi - (\beta+1)\zeta\phi^2}{b\beta\zeta + [\beta(1-\zeta)+b\beta\zeta]\phi + \beta(1-\zeta)\phi^2}\right)\right]^+, \tag{2.27}$$

$$\underline{R}_{nk}^{\text{sec},\mathcal{R}} = \left[\log_2\left(\frac{(b+1)\beta\zeta + [1-(b+1)\beta]\zeta\phi - \zeta\phi^2}{(b+1)\beta\zeta + (b+1)\beta(1-\zeta)\phi}\right)\right]^+, \tag{2.28}$$

where $b = (M-1)\rho + 1/P_T$ and $\eta = q/p = \beta(1/\phi - 1)/(1-\beta)$ was used. In the following, we first investigate for what values of α a non-zero ergodic secrecy rate can be achieved.

Impact of α: Let us denote the upper limit for α such that a positive secrecy rate can be achieved as α_{sec}. For the $\mathcal{N}$-method and the $\mathcal{R}$-method, we obtain from (2.27) and (2.28), respectively, positive secrecy rates if $\alpha < \alpha_{\text{sec}}^{\Psi}$, $\Psi \in \{\mathcal{N}, \mathcal{R}\}$, with

$$\alpha_{\text{sec}}^{\mathcal{N}} = \frac{a^2(1-\beta)}{ab(1-\beta)+c} \overset{\beta\to 0}{=} \frac{a}{b+c/a} = \frac{1+\rho(M-1)}{1/P_T + \rho(M-1) + c/a} \tag{2.29}$$

and

$$\alpha_{\text{sec}}^{\mathcal{R}} = \frac{a^2(1-\beta)}{a(b+1)(1-\beta)+c} \overset{\beta\to 0}{=} \frac{a}{b+1+c/a} = \frac{1}{1+1/[P_T(\rho(M-1)+1)] + c/a^2}. \tag{2.30}$$

In both cases, $\alpha_{\text{sec}}^{\Psi}$ is obtained for $\phi \to 0$, i.e., almost the entire transmit power is allocated to AN precoding. For both methods, α_{sec} is monotonically decreasing in β. Furthermore, we always have $\alpha_{\text{sec}}^{\mathcal{R}} < \alpha_{\text{sec}}^{\mathcal{N}}$, i.e., the $\mathcal{N}$-method can tolerate a larger number of eavesdropper antennas than the $\mathcal{R}$-method at the expense of a higher complexity in calculating the AN precoding matrix. The robustness of both AN precoding matrix designs can be improved by increasing the transmit power P_T. However, based on (2.29) and (2.30) it can be shown that even for $P_T \to \infty$, the maximum values of α that yield a non-zero ergodic secrecy rate are limited as

$\alpha_{\text{sec}}^{\mathcal{N}} \leq 4/3$ and $\alpha_{\text{sec}}^{\mathcal{R}} \leq 1$ regardless of the choice of M and ρ. We note that for a single-cell system with a single user, it was shown in [27] that the $\mathcal{N}$-method can achieve non-zero secrecy rate for $\alpha < 2$. The smaller number of tolerable eavesdropper antennas in the considered massive MIMO system are caused by the suboptimal MF precoding at the BS, which was chosen for complexity reasons. More sophiscated precoding techniques will be considered in Chapter 3.

Impact of ϕ: Eqs. (2.27) and (2.28) reveal that zero secrecy rate results for $\phi = \phi_0 = 0$ and for a second value $\phi = \phi_1^{\Psi}$, $0 < \phi_1^{\Psi} < 1$, where $\Psi \in \{\mathcal{N}, \mathcal{R}\}$. Specifically, ϕ_1^{Ψ} is given by

$$\phi_1^{\mathcal{N}} = 1 - \frac{\alpha a(1-\beta)(b+1)}{a^2(1-\beta)(1+\alpha/a) - c\alpha} \tag{2.31}$$

$$\phi_1^{\mathcal{R}} = 1 - \frac{\alpha a(1-\beta)(b+1)}{a^2(1-\beta) - c\alpha} \tag{2.32}$$

where $\phi_1^{\Psi} < 1$ follows from the condition $\beta < 1 - c\alpha/a^2$ which is required for the validity of the upper bound on the ergodic secrecy capacity in (2.16). For $\phi = 0$, all power is allocated to AN precoding and no power is left for information transmission. On the other hand, for $\phi = \phi_1^{\Psi}$, the amount of AN generated is not sufficient to prevent the eavesdropper from decoding the transmitted signal. This suggests that for $\alpha < \alpha_{\text{sec}}^{\Psi}$, $\Psi \in \{\mathcal{N}, \mathcal{R}\}$, there exists an optimal ϕ, $0 < \phi < \phi_1^{\Psi}$, which maximizes the achievable ergodic secrecy rate. The values of the optimal ϕ can be obtained from (2.27) and (2.28) as

$$\phi_{\mathcal{N}}^* = \frac{-(b\beta + b\zeta) + \sqrt{b(b+1)(\zeta - b\beta + \beta\zeta + b\beta\zeta)}}{1 + b + \beta - b\zeta}, \tag{2.33}$$

$$\phi_{\mathcal{R}}^* = \frac{-\zeta + \sqrt{\zeta - \beta - b\beta + \zeta\beta + b\beta\zeta}}{1 - \zeta}. \tag{2.34}$$

Impact of β: It can be shown from (2.33) and (2.34) that for both the $\mathcal{N}$ and $\mathcal{R}$ methods the optimal ϕ is a monotonically increasing function of $\beta \in (0, 1 - c\alpha/a^2)$. Thus, as the number of MTs in the cell increase, the amount of power allocated to AN precoding decreases. This can be explained by the fact that as β increases, the transmit power per MT used for information transmission, $\phi P_T/K$, decreases. To compensate for this effect, a larger ϕ is necessary. On the other hand, the ergodic secrecy rates for both the $\mathcal{N}$ and $\mathcal{R}$ methods are decreasing functions of $\beta \in (0, 1 - c\alpha/a^2)$, cf. (2.27), (2.28), i.e., as expected, for a given number of users the ergodic secrecy rates increase with increasing number of BS antennas. Surprisingly, this property does not necessarily hold in case of pilot contamination, cf. Section 2.5.

2.4.3 Secrecy Outage Probability Analysis

In delay limited scenarios, where one codeword spans only one channel realization, outages are unavoidable since Alice does not have the CSI of the eavesdropper channel and the secrecy outage probability has to be used to characterize the performance of the system instead of the ergodic rate. For the considered multi-cell massive MIMO system, the rate of the desired user, R_{nk}, becomes deterministic as $N_T \to \infty$, but the instantaneous capacity of the eavesdropper channel remains a random variable. A secrecy outage occurs whenever the target secrecy rate R_0 exceeds the actual instantaneous secrecy rate. Thus, the secrecy outage probability of the k^{th} MT in the local cell is given by

$$\varepsilon_{\text{out}} = \Pr\{R_{nk} - \log_2(1+\gamma_E) \le R_0\} = \Pr\{\gamma_E \ge 2^{R_{nk}-R_0} - 1\} = 1 - F_{\gamma_E}(2^{R_{nk}-R_0} - 1), \tag{2.35}$$

where $\gamma_E = p\mathbf{f}_{nk}^H \mathbf{G}_{nE}^H \mathbf{X}^{-1} \mathbf{G}_{nE} \mathbf{f}_{nk}$ and $F_{\gamma_E}(x)$ is given in Appendix A.2. A closed-form upper bound on the secrecy outage probability is obtained by replacing R_{nk} with $\underline{R}_{nk}^{\Psi} = \log_2(1 + \gamma_{nk}^{\Psi})$ with γ_{nk}^{Ψ} given in (2.24)/(2.25).

2.5 Performance Analysis for Pilot Contamination

In this section, we analyze the performance of the considered multi-cell massive MIMO system for the case of pilot contamination. To this end, we simplify the lower bound on the achievable ergodic rate expression derived in Section 2.3.2 for the case of pilot contamination, derive insightful and tight lower bounds on the ergodic secrecy rate, and provide a closed-form expression for the secrecy outage probability.

2.5.1 Lower Bound on the Achievable Ergodic Rate

The lower bound on the achievable ergodic rate of the users derived in Section 2.3.2 is also applicable in case of pilot contamination. Thus, in a first step, we characterize the four expectations/variances in the SINR expression in (2.12).

Expressing the small-scale fading vector as $\mathbf{h}_{nn}^k = \hat{\mathbf{h}}_{nn}^k + \tilde{\mathbf{h}}_{nn}^k$, cf. Section 2.2, the denominator of (2.12) can be rewritten as (we omit the path-loss for the moment)

$$\mathbb{E}[\mathbf{h}_{nn}^k \mathbf{f}_{nk}] = \mathbb{E}\left[\|\hat{\mathbf{h}}_{nn}^k\| + \tilde{\mathbf{h}}_{nn}^k \frac{(\hat{\mathbf{h}}_{nn}^k)^H}{\|\hat{\mathbf{h}}_{nn}^k\|} \right] = \mathbb{E}[\|\hat{\mathbf{h}}_{nn}^k\|] = \sqrt{\frac{p_\tau \tau \beta_{nn}^k}{1 + p_\tau \tau \sum_{m=1}^M \beta_{nm}^k}} \mathbb{E}[x], \quad (2.36)$$

where $x^2 \sim \chi_{2N_T}^2$, cf. Lemma 2.2. Furthermore, we observe from (2.2) that, at the local BS, the channel estimate for the k^{th} MT in the local cell involves the sum of all channel vectors between the local BS and the k^{th} MTs in all cells weighted with scaling factors $\frac{\sqrt{p_\tau \tau \beta_{nm}^k}}{1 + p_\tau \tau \sum_{l=1}^M \beta_{nl}^k}$. Thus, the transmit beamforming vector for the k^{th} MT in the local cell is also affected by the channel vectors between the local BS and the k^{th} MTs in all other cells. This is the fundamental problem introduced by pilot contamination. Using this observation, the interference caused by the k^{th} MT in the m^{th} cell to the local cell (i.e., the component of the third term of the denominator in (2.12) with $l = k$) is given by

$$\begin{aligned}\mathbb{E}[|\mathbf{h}_{mn}^{k}\mathbf{f}_{mk}|^2] &= \mathbb{E}\big[\|\hat{\mathbf{h}}_{mn}^{k}\|^2\big] + \mathbb{E}\left[\frac{\hat{\mathbf{h}}_{mn}^{k}}{\|\hat{\mathbf{h}}_{mn}^{k}\|}(\tilde{\mathbf{h}}_{mn}^{k})^H\tilde{\mathbf{h}}_{mn}^{k}\frac{(\hat{\mathbf{h}}_{mn}^{k})^H}{\|\hat{\mathbf{h}}_{mn}^{k}\|}\right] \\ &= \frac{p_\tau \tau \beta_{mn}^{k}}{1 + p_\tau \tau \sum_{l=1}^{M}\beta_{ml}^{k}}\mathbb{E}[x^2] + \frac{1 + p_\tau \tau \sum_{l \neq n}\beta_{ml}^{k}}{1 + p_\tau \tau \sum_{l=1}^{M}\beta_{ml}^{k}}\mathbb{E}[y^2], \qquad (2.37)\end{aligned}$$

where $y^2 \sim \chi_2^2$, cf. Lemma 2.1. Exploiting now (2.36) and (2.37) and the definition of variance, i.e., $\text{var}[x] = \mathbb{E}[x^2] - \mathbb{E}^2[x]$, we obtain for the signal leakage term in (2.12)

$$\text{var}[\mathbf{h}_{nn}^{k}\mathbf{f}_{nk}] = \frac{p_\tau \tau \beta_{nn}^{k}}{1 + p_\tau \tau \sum_{m=1}^{M}\beta_{nm}^{k}}\text{var}[x] + \frac{1 + p_\tau \tau \sum_{m \neq n}\beta_{nm}^{k}}{1 + p_\tau \tau \sum_{m=1}^{M}\beta_{nm}^{k}}\mathbb{E}[y^2]. \qquad (2.38)$$

Furthermore, the interference from the l^{th} MT, where $l \neq k$, in the adjacent (i.e., non-local) cells is given by

$$\mathbb{E}[|\mathbf{h}_{mn}^{k}\mathbf{f}_{ml}|^2] = \mathbb{E}[y^2], \qquad (2.39)$$

as each $\mathbf{f}_{ml}$, $\forall l \neq k$, has unit norm and is independent of $\mathbf{h}_{mn}^{k}$. While the terms calculated in (2.36)-(2.39) are identical for the $\mathcal{N}$ and $\mathcal{R}$ methods, the AN leakage depends on the AN precoding matrix design. In particular, for the $\mathcal{N}$-method, the AN is designed to lie in the NS of the estimated channels from each BS to all K MTs in its own cell, which is also a scaled version of the estimated channels from each BS to all K MTs in the local cell due to pilot contamination, cf. (2.3). This implies that all $\hat{\mathbf{h}}_{ml}^{k}, \forall l$ are aligned, cf. Section 2.2.2. Hence, the AN leakage is obtained as

$$\mathbb{E}[|\mathbf{h}_{mn}^{k}\mathbf{a}_{mi}|^2] = \mathbb{E}[\tilde{\mathbf{h}}_{mn}^{k}\mathbf{a}_{mi}\mathbf{a}_{mi}^{H}(\tilde{\mathbf{h}}_{mn}^{k})^H] = \frac{1 + p_\tau \tau \sum_{l \neq n}\beta_{ml}^{k}}{1 + p_\tau \tau \sum_{l=1}^{M}\beta_{ml}^{k}}\mathbb{E}[y^2], \forall m, \qquad (2.40)$$

by exploiting $\mathbb{E}[|\hat{\mathbf{h}}_{mm}^{k}\mathbf{a}_{mi}|^2] = 0$ for $\mathcal{N}$-method and the independence of $\mathbf{a}_{mi}$, $\forall i$, and $\tilde{\mathbf{h}}_{mn}^{k}$. On the other hand, for the $\mathcal{R}$-method, the AN is generated randomly, such that $\mathbb{E}[|\mathbf{h}_{mn}^{k}\mathbf{a}_{mi}|^2] = \mathbb{E}[y^2]$, since the $\mathbf{a}_{mi}$, $\forall i$, have unit norm and are independent of $\mathbf{h}_{mn}^{k}$.

Plugging all intermediate results derived in this section so far into (2.12), we obtain $\gamma_{nk}^{\mathcal{N}} =$

$$\frac{\lambda_{nk}\mathbb{E}^2[x]}{\lambda_{nk}\mathrm{var}[x] + \sum_{m=1}^{M}\left(\mu_{mk} + \eta\sum_{i=1}^{N_T-K}\mu_{mk} + \sum_{l\neq k}\beta_{mn}^{k}\right)\mathbb{E}[y^2] + \sum_{m\neq n}\lambda_{mk}\mathbb{E}[x^2] + \frac{K}{\phi P_T}} \tag{2.41}$$

and $\gamma_{nk}^{\mathcal{R}} =$

$$\frac{\lambda_{nk}\mathbb{E}^2[x]}{\lambda_{nk}\mathrm{var}[x] + \sum_{m=1}^{M}\left(\mu_{mk} + \eta\sum_{i=1}^{N_T-K}\beta_{mn}^{k} + \sum_{l\neq k}\beta_{mn}^{k}\right)\mathbb{E}[y^2] + \sum_{m\neq n}\lambda_{mk}\mathbb{E}[x^2] + \frac{K}{\phi P_T}}, \tag{2.42}$$

where $\lambda_{mk} = \beta_{mn}^{k}\frac{p_\tau\tau\beta_{mn}^{k}}{1+p_\tau\tau\sum_{l=1}^{M}\beta_{ml}^{k}}$ and $\mu_{mk} = \beta_{mn}^{k}\frac{1+p_\tau\tau\sum_{l\neq n}\beta_{ml}^{k}}{1+p_\tau\tau\sum_{l=1}^{M}\beta_{ml}^{k}}$. Adopting now the same simplified interference model as in Section 2.4, the term $\sum_{m=1}^{M}\mu_{mk}$ in (2.41) and (2.42) can be simplified as $1-\lambda+(M-1)\rho(1-\rho\lambda) = a - c\lambda$. Other terms can be simplified in the same way. By combining all terms together, (2.41) and (2.42) can be further simplified for large N_T, the corresponding lower bound on the achievable ergodic rates are given by

$$\underline{R}_{nk}^{\mathcal{N}} = \log_2\left(1 + \frac{\lambda}{(a-c\lambda)(1-\beta)\eta + a\beta + (M-1)\rho^2\lambda + \frac{\beta}{\phi P_T}}\right) \tag{2.43}$$

and

$$\underline{R}_{nk}^{\mathcal{R}} = \log_2\left(1 + \frac{\lambda}{a(1-\beta)\eta + a\beta + (M-1)\rho^2\lambda + \frac{\beta}{\phi P_T}}\right), \tag{2.44}$$

where $\lambda = \frac{p_\tau\tau}{1+p_\tau\tau a}$. From (2.43) and (2.44) we observe that $\underline{R}_{nk}^{\mathcal{N}} > \underline{R}_{nk}^{\mathcal{R}}$ always holds but the performance difference diminishes if $a/c \gg \lambda$. We note that for both AN precoding matrix designs the powers of the inter-cell interference are proportional to $a - 1 = (M-1)\rho$. Furthermore, for the $\mathcal{N}$-method and the $\mathcal{R}$-method, the AN leakage is proportional to $(1 - c/a\lambda)\eta$ and η, respectively. Therefore, $a/c \gg \lambda$ implies that the inter-cell interference are much stronger (but with a weaker ρ to have $a \gg c$) than the AN leakage and/or the pilot power p_τ is not sufficiently large to prevent AN leakage for the $\mathcal{N}$-method. Furthermore, for $\beta \to 0$, we obtain $\underline{R}_{nk}^{\mathcal{N}} = \log_2(1+\lambda/[(a-c\lambda)\eta+(M-1)\rho^2\lambda])$ and $\underline{R}_{nk}^{\mathcal{R}} = \log_2(1+\lambda/[a\eta+(M-1)\rho^2\lambda])$, i.e., in the asymptotic regime where the number of users is constant but the number of BS antennas increases without bound, the performance for both AN precoding matrix designs is limited by both AN leakage and pilot contamination.

Since the ergodic capacity of the eavesdropper is not affected by the imperfect CSI at the local BS, a lower bound on the ergodic secrecy rate for pilot contamination can be calculated from (2.7), (2.8), and (2.43)/(2.44).

2.5.2 Impact of System Parameters on Ergodic Secrecy Rate

To gain more insight, we employ again the upper bound on the ergodic capacity of the eavesdropper provided in Theorem 2.2. Combining (2.7), (2.16), (2.43), and (2.44), we obtain simple lower bounds for the ergodic secrecy rate for the $\mathcal{N}$ and $\mathcal{R}$ methods as $\underline{R}_{nk}^{\mathrm{sec},\mathcal{N}} = \Bigg[\log_2$

$$\left(\frac{(b+1-c\lambda)\beta\zeta + [(\beta+1)c\lambda - (b+1-c\lambda)\beta]\zeta\phi - \zeta(\beta+1)c\lambda\phi^2}{(b+1-c\lambda)\beta\zeta + [(\beta c+c-1)\lambda\zeta + (b+1-c\lambda)\beta(1-\zeta)]\phi + (1-\zeta)(\beta c+c-1)\lambda\phi^2}\right)\Bigg]^+, \tag{2.45}$$

and

$$\underline{R}_{nk}^{\mathrm{sec},\mathcal{R}} = \left[\log_2\left(\frac{(b+1)\beta\zeta + [c\lambda - (b+1)\beta]\zeta\phi - \zeta c\lambda\phi^2}{(b+1)\beta\zeta + [(c-1)\lambda\zeta + (b+1)\beta(1-\zeta)]\phi + (1-\zeta)(c-1)\lambda\phi^2}\right)\right]^+, \tag{2.46}$$

respectively.

In the following, we investigate the impact of the system parameters on the ergodic secrecy rate in detail.

Impact of α: Similar to the perfect training case we investigate in the following the upper limit for α such that a positive secrecy rate can be achieved. We observe from (2.45) and (2.46) that a non-zero secrecy rate can be achieved as long as $\alpha < \alpha_{\mathrm{sec}}^{\Psi}$ holds where

$$\alpha_{\mathrm{sec}}^{\mathcal{N}} = \frac{a^2(1-\beta)\lambda}{a(1-\beta)(1+b-c\lambda)+c\lambda} \overset{\beta\to 0}{=} \frac{a^2\lambda}{a(1+b-c\lambda)+c\lambda}, \tag{2.47}$$

$$\alpha_{\mathrm{sec}}^{\mathcal{R}} = \frac{a^2(1-\beta)\lambda}{a(1-\beta)(1+b)+c\lambda} \overset{\beta\to 0}{=} \frac{a^2\lambda}{a(1+b)+c\lambda}. \tag{2.48}$$

Eqs. (2.47) and (2.48) reveal that the robustness of the considered multi-cell MIMO system to eavesdropping is monotonically decreasing with increasing number of MTs in the system. On the other hand, allocating more resources to training, i.e., increasing λ by increasing the pilot power, p_τ, or the pilot sequence duration, τ, leads to a higher robustness against eavesdropping, i.e., a larger number of eavesdropper antennas can be tolerated. Furthermore, as expected, $\alpha_{\mathrm{sec}}^{\mathcal{N}} > \alpha_{\mathrm{sec}}^{\mathcal{R}}$, i.e., the more complex $\mathcal{N}$-method is more robust to eavesdropping than the simple $\mathcal{R}$ method. However, $\alpha_{\mathrm{sec}}^{\mathcal{R}}$ approaches $\alpha_{\mathrm{sec}}^{\mathcal{N}}$ if both c and λ are small, i.e., both methods have a similar robustness to eavesdropping in case of strong pilot contamination but a small value of ρ, since, in this case, the $\mathcal{N}$-method can no longer avoid AN leakage. We also note that, as expected, since $\lambda < 1$ always holds, for $\mathcal{R}$-method, the maximum tolerable number of eavesdropper antennas in case of pilot contamination is always smaller than that in case of perfect training. Surprisingly, on the other hand, for the $\mathcal{N}$-method, the maximum tolerable number of eavesdropper antennas for pilot contamination is possible to be larger than that for perfect training, if $\lambda > \frac{b+1}{b+c}$, cf. (2.29), (2.30), and (2.47), (2.48). This mainly attributes to the inter-cell AN leakage suppression due to pilot contamination, cf. Lemma 2.2 and (2.40). In particular, the channel estimates in adjacent cells also involve the inter-cell interference channel vector between the adjacent BS and MTs in the local cell. Therefore, the AN emitted in adjacent cells is affected by the inter-cell interference channels. In this regard, pilot contamination is beneficial for improving the system performance.

Impact of ϕ: Similar to the case of perfect training, the ergodic secrecy rate for both AN precoding matrix designs becomes zero for $\phi = \phi_0 = 0$ also for the case of pilot contamination, cf. (2.45) and (2.46), since zero power is allocated to information transmission in this case. A second zero of the ergodic secrecy rate occurs for $\phi = \phi_1^{\Psi}$, $0 < \phi_1^{\Psi} < 1$, where $\Psi \in \{\mathcal{N}, \mathcal{R}\}$. ϕ_1^{Ψ} is obtained from (2.45) and (2.46) as

$$\begin{aligned} \phi_1^{\mathcal{N}} &= 1 - \frac{\alpha a(\beta-1)((b+1)\beta + \lambda(c-1))}{\lambda(a(a+c\alpha)\beta^2 + (-a^2+\alpha a + c\alpha)\beta - a\alpha(c-1))} && (2.49) \\ \phi_1^{\mathcal{R}} &= 1 - \frac{\alpha a(\beta-1)((b+1)\beta + \lambda(c-1))}{\lambda(a^2\beta^2 + (-a^2 + a\alpha(c-1) + c\alpha)\beta - a\alpha(c-1))}. && (2.50) \end{aligned}$$

Furthermore, assuming $\alpha < \alpha_{\text{sec}}^{\Psi}$ and taking the derivatives of (2.45) and (2.46) with respect to ϕ and setting them to zero, we obtain the optimal power allocation factors for the $\mathcal{N}$ and $\mathcal{R}$ methods as

$$\begin{aligned} \phi_{\mathcal{N}}^* = & \frac{-\sqrt{(b+1-c\lambda)((-1+c)\lambda + (b+1)\beta)\beta((\beta c + c\zeta)\lambda + (-1+\zeta)\beta(b+1))\lambda}}{(-\lambda c^2\beta^2 + ((2-2c-\zeta)\lambda + (-1+\zeta)(b+1))\beta - c\lambda(-1+c))\lambda} \\ & + \frac{(-c^2\lambda^2 + (b+1)\lambda)\beta^2 + ((-c-\zeta+1)c\lambda^2 + ((\zeta-1+c)b + \zeta - 1 + c)\lambda)\beta}{(-\lambda c^2\beta^2 + ((2-2c-\zeta)\lambda + (-1+\zeta)(b+1))\beta - c\lambda(-1+c))\lambda} \quad (2.51) \end{aligned}$$

and

$$\phi^*_{\mathcal{R}} = \frac{-\sqrt{\lambda((-1+c)\lambda+(b+1)\beta)(b+1)(c\zeta\lambda+(-1+\zeta)\beta(b+1))\beta}}{\lambda((-1+\zeta)\beta(b+1)-c\lambda(-1+c))} + \frac{((\zeta-1+c)b+\zeta-1+c)\lambda\beta}{\lambda((-1+\zeta)\beta(b+1)-c\lambda(-1+c))}. \tag{2.52}$$

Impact of β: Based on (2.51) and (2.52) it can be shown that, similar to the case for perfect training, for pilot contamination, the optimal $\phi^*_{\mathcal{N}}$ and $\phi^*_{\mathcal{R}}$ are monotonically increasing in β. Furthermore, in Section 2.4, we found that, for perfect training, the ergodic secrecy rate is monotonically increasing for decreasing β. However, for a given ϕ, it can be shown based on (2.45) and (2.46) that this is no longer true in case of pilot contamination. In other words, if ϕ and the number of users K are fixed, in case of pilot contamination, the ergodic secrecy rate is not maximized by making the number of BS antennas, N_T, exceedingly large (i.e., $N_T \gg K$ such that $\beta \to 0$). Instead, there is an optimal finite number of BS antennas. We will investigate this issue numerically in Section 2.6.

Impact of λ: Pilot contamination impacts the ergodic secrecy rate via λ, where smaller values of λ imply that the MTs expend less resources for uplink training (i.e., they employ a smaller pilot power p_τ and/or a shorter pilot sequence length, τ). First, we observe from (2.45) and (2.46) that both $\underline{R}^{\text{sec},\mathcal{N}}_{nk}$ and $\underline{R}^{\text{sec},\mathcal{R}}_{nk}$ are increasing functions of λ, i.e., as expected, if the MTs employ a higher pilot power and/or a longer pilot sequence for channel estimation, the ergodic secrecy rate improves. Furthermore, α_{sec} is an increasing function of λ, i.e., a higher uplink training power and/or longer pilot sequence lengths increase the operating region of the system where a non-zero secrecy rate can be achieved.

On the other hand, for a given coherence interval T, fixed transmit power P_T, and fixed pilot power p_τ, the fraction of time allocated for training τ/T (and as a consequence λ) can be optimized for maximization of the net ergodic secrecy rate given by $(1-\tau/T)R_{nk}^{\text{sec},\Psi}$, $\Psi \in \{\mathcal{N}, \mathcal{R}\}$. We assume that the channels are constant within one coherence interval but change from one coherence interval to the next. We also emphasize that by using the (net) ergodic secrecy rate as a performance measure, we implicitly assume coding over many coherence intervals. For small τ, the factor $(1-\tau/T)$ is large but the ergodic secrecy rate, $R_{nk}^{\text{sec},\Psi}$, is small because of the unreliable channel estimation. On the other hand, for large τ, the factor $(1-\tau/T)$ is small but the ergodic secrecy rate, $R_{nk}^{\text{sec},\Psi}$, is large because of the more accurate channel estimation. Hence, τ can be optimized for optimal performance [68]. The optimization of τ will be studied numerically in Fig. 2.9 in Section 2.6.

2.5.3 Secrecy Outage Probability Analysis

Plugging (2.43) and (2.44) into the secrecy outage probability expression derived in (2.35), we obtain an upper bound for the secrecy outage probability for the case of pilot contamination as

$$\overline{\varepsilon}_{\text{out}}^{\Psi} = 1 - F_{\gamma_E}\left(2^{\underline{R}_{nk}^{\Psi} - R_0} - 1\right), \tag{2.53}$$

where $\Psi \in \{\mathcal{N}, \mathcal{R}\}$.

2.6 Numerical Examples

In this section, we evaluate the secrecy performance of the considered multi-cell massive MIMO systems based on the analytical expressions derived in Sections 2.2-2.5 and via Monte-Carlo simulation. We consider a system with $M = 7$ hexagonal cells and adopt the simplified path-loss model, i.e., the severeness of the inter-cell interference is characterized by parameter ρ only. The Monte-Carlo simulation results for the ergodic secrecy rate of the k^{th} MT in the local cell are based on (2.7) where the achievable ergodic rate R_{nk} is obtained from (2.9) and the ergodic secrecy capacity of the eavesdropper is obtained from (2.8). Thereby, the expected values in (2.9) and (2.8) were evaluated by averaging over 5000 random channel realizations. The Monte-Carlo simulation results for the outage probability are obtained from $\varepsilon_{\text{out}} = \Pr\{R_{nk} - \log_2(1 + \gamma_E) \leq R_0\}$, which was evaluated again based on 5000 random channel realizations. The values of all relevant system parameters are provided in the captions of the figures.

2.6.1 Ergodic Secrecy Rate and Secrecy Outage Probability

For the results shown in this section, we adopt a fixed power allocation factor of $\phi = 0.75$. The optimization of ϕ will be addressed in the next subsection.

In Fig. 2.2, we verify the derived analytical expressions for the ergodic capacity of the eavesdropper which seeks to decode the information intended for the k^{th} MT in the local cell. The analytical results were generated with (2.13) while the upper bound results were computed with (2.16). The vertical dashed lines denote $\beta = 1 - c\alpha/a^2$. Fig. 2.2 reveals that for $\beta < 1 - c\alpha/a^2$, the upper bound is very tight. For $1 - c\alpha/a^2 < \beta < 1 - \alpha/M$, the upper bound is not applicable, although the ergodic capacity of the eavesdropper is still finite, cf. Theorem 2.2 and Remark 2.1. For $\beta \rightarrow 1 - \alpha/M$, the ergodic capacity of the eavesdropper tends to infinity since $\mathbf{X}$ becomes singular. Furthermore, we observe from Fig. 2.2 that increasing inter-cell interference (i.e., larger inter-cell interference factors, ρ) has a negative effect on the ergodic capacity of the eavesdropper, whereas as expected, the eavesdropper can improve his performance by adding more antennas, N_E (i.e., by increasing α). Moreover,

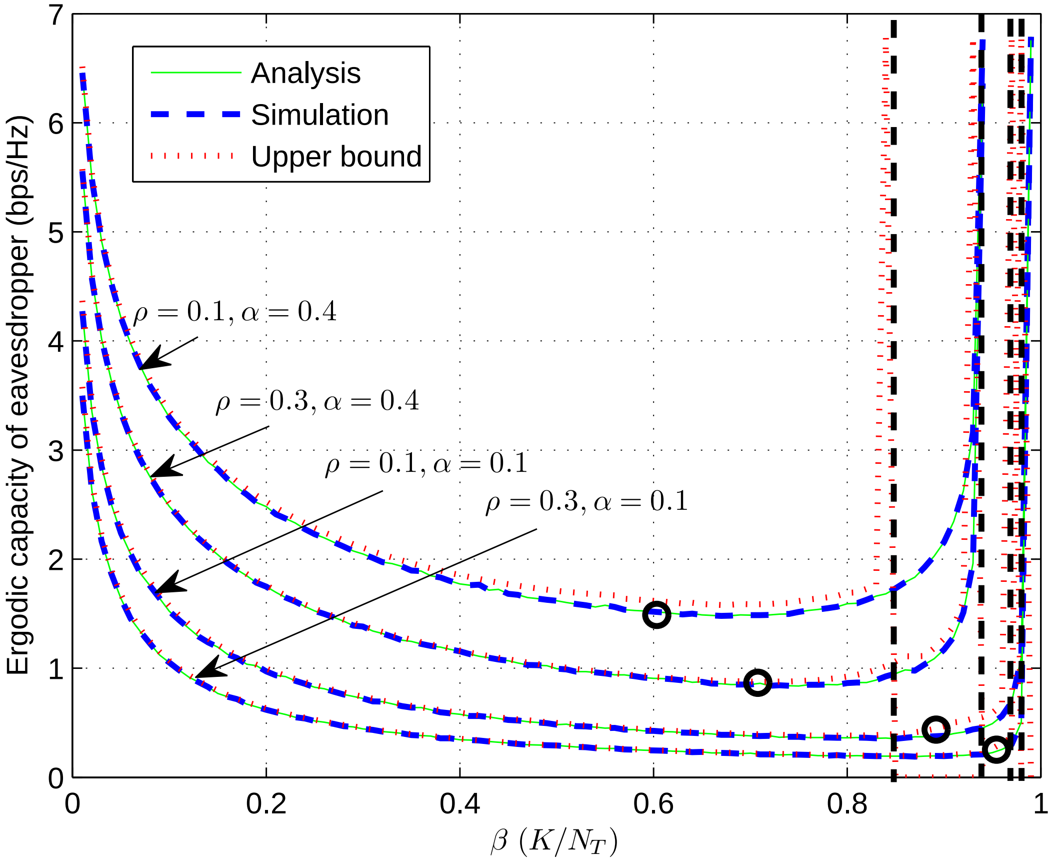

Figure 2.2: Ergodic capacity of the eavesdropper seeking to decode the information intended for the k^{th} MT in the local cell vs. the normalized number of MTs in the cell, β, for a system with total transmit power $P_T = 10$ dB, $M = 7$, $\phi = 0.75$, and $N_T = 100$.

Fig. 2.2 confirms that the ergodic capacity of the eavesdropper is monotonically decreasing in β in the interval $(0, 1 - \sqrt{c\alpha}/a)$ and monotonically increasing in β in the interval $(1 - \sqrt{c\alpha}/a, 1 - c\alpha/a^2)$. The resulting minimum of the ergodic capacity of the eavesdropper at $\beta = 1 - \sqrt{c\alpha}/a$ is denoted by a black circle in Fig. 2.2.

In Fig. 2.3, for the case of perfect training, we show the ergodic secrecy rate vs. the number of BS antennas (subfigure (a)) and the secrecy outage probability vs. the target secrecy rate R_0 (subfigure (b)) for the k^{th} MT in the local cell. Results for both considered AN precoding matrix designs are shown. In subfigure (a), lower bound I was obtained based on (2.7), (2.13), (2.24), and (2.25) and lower bound II was obtained with (2.27) and (2.28). In subfigure (b), the upper bound was obtained with (2.35). Fig. 2.3 reveals that the derived bounds for the ergodic secrecy rate and the secrecy outage probability are accurate. As expected, for the ergodic secrecy rate, lower bound I is somewhat tighter than lower bound II. Furthermore, increasing the number of BS antennas N_T improves both the ergodic secrecy rate as well as the secrecy outage probability. Moreover, as expected, the $\mathcal{N}$-method for generation of the AN precoding matrix always outperforms the $\mathcal{R}$-method as the $\mathcal{N}$-method avoids intra-cell AN leakage.

In Fig. 2.4, we show the same performance metrics as in Fig. 2.3, however, now for the case of pilot contamination. In subfigure (a), lower bound I was obtained based on (2.7), (2.13), (2.43), and (2.44), whereas lower bound II was obtained with (2.45) and (2.46). In subfigure (b), the upper bound was obtained with (2.53). Similar to the case of perfect training, the derived bounds on the ergodic secrecy rate and the secrecy outage probability are very tight. A comparison of Figs. 2.3 and 2.4 reveals that pilot contamination causes a significant performance degradation in terms of both ergodic secrecy rate and secrecy outage probability. Furthermore, unlike for the case of perfect training, for pilot contamination, the ergodic secrecy rate is not monotonically increasing in N_T but has a unique maximum for both AN precoding matrix designs.

2.6.2 Optimal Power Allocation

In this subsection, we investigate the optimization of power allocation factor ϕ and illustrate its impact on the ergodic secrecy rate.

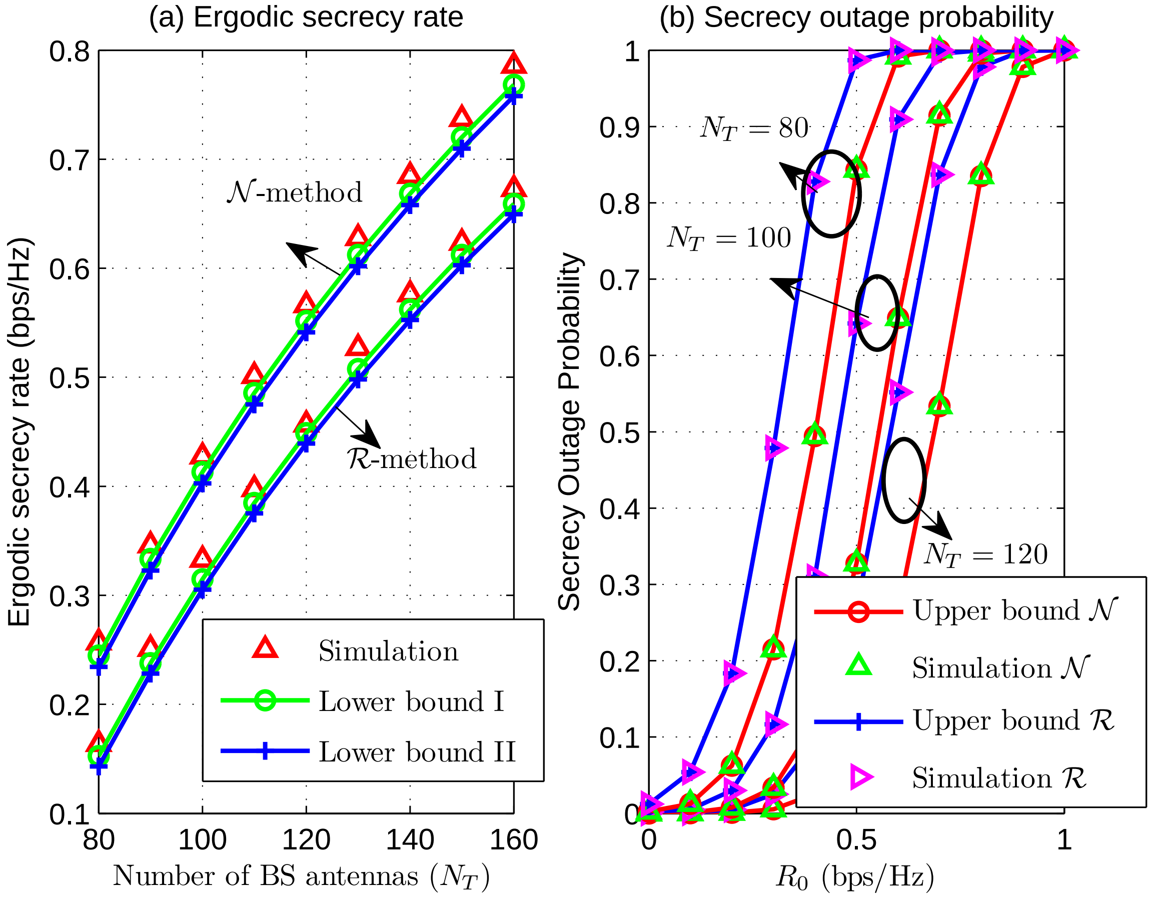

Figure 2.3: Ergodic secrecy rate and outage probability for perfect training, $M = 7$, $P_T = 10$ dB, $K = 10$, $\rho = 0.3$, $\alpha = 0.1$, and $\phi = 0.75$.

Figs. 2.5 and 2.6 show the ergodic secrecy rates of the k^{th} MT in the local cell as functions of ϕ for the cases of perfect training and pilot contamination, respectively. The ergodic secrecy rate curves were obtained via Monte Carlo simulation and various values of α and β are considered. The optimal values for ϕ obtained with (2.33)/(2.34) (for perfect training) and (2.51)/(2.52) (for pilot contamination) are denoted by black circles. As expected from our discussions in Sections 2.4 and 2.5, Figs. 2.5 and 2.6 show that, for both the $\mathcal{N}$ and the $\mathcal{R}$ AN precoding matrix desigs, the optimal ϕ^* is decreasing in α, i.e., the system should allocate more power to AN if the eavesdropper

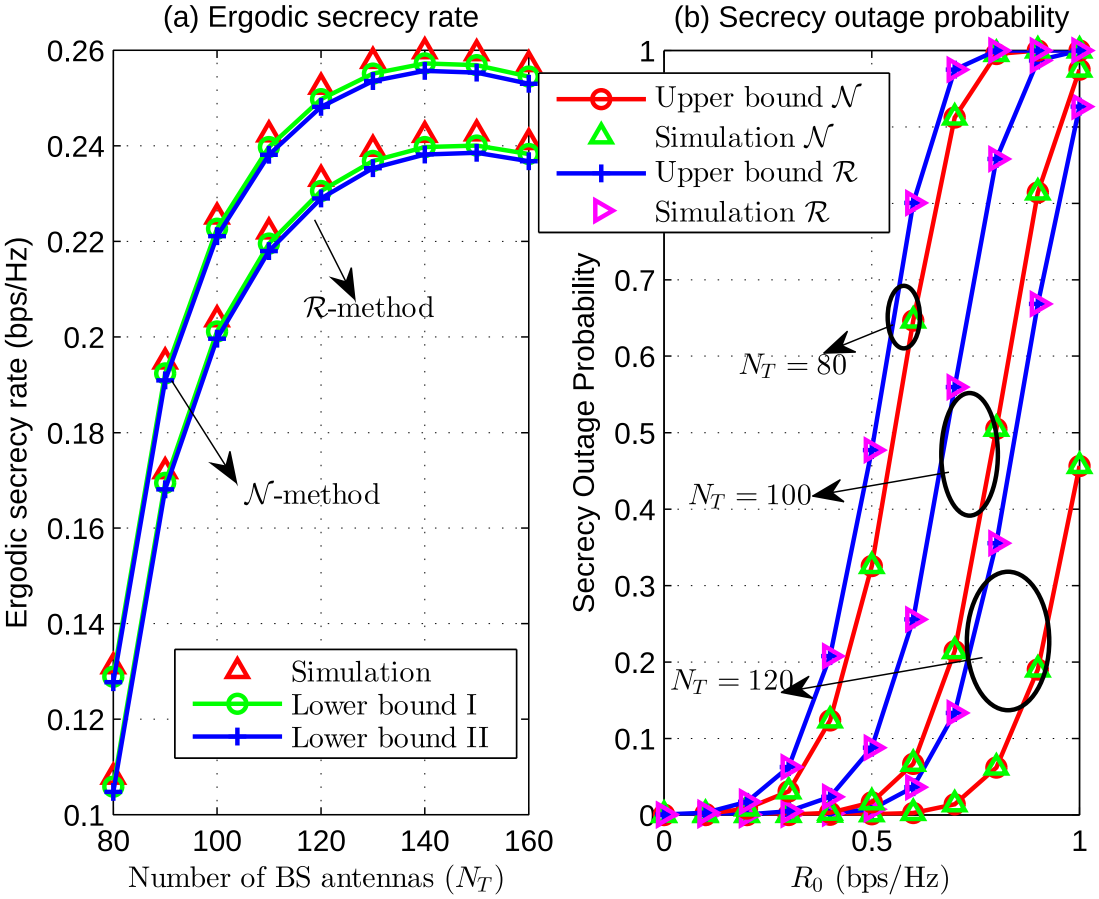

Figure 2.4: Ergodic secrecy rate and outage probability for pilot contamination, $M = 7$, $P_T = 10$ dB, $K = 10$ MTs, $\rho = 0.1$, $\alpha = 0.1$, $\phi = 0.75$, $\tau = K$, and $p_\tau = P_T/K$.

is becoming stronger, and increasing in β, i.e., less power should be allocated to AN if the number of users increases. For $\alpha = 0.4$, no results are shown for the case of pilot contamination in Fig. 2.6 since the corresponding ergodic secrecy rates are zero for all choices of ϕ, i.e., $\alpha > \alpha_{\text{sec}}$ holds in this case.

In Fig. 2.7, we depict the ergodic secrecy rate and the optimal power allocation factor, ϕ^*, as functions of the normalized number of MTs in each cell, β. Thereby, the ergodic secrecy rate is calculated using the optimal ϕ^*, which was obtained based on the analytical results in Sections 2.4 and 2.5 for the case of perfect training and

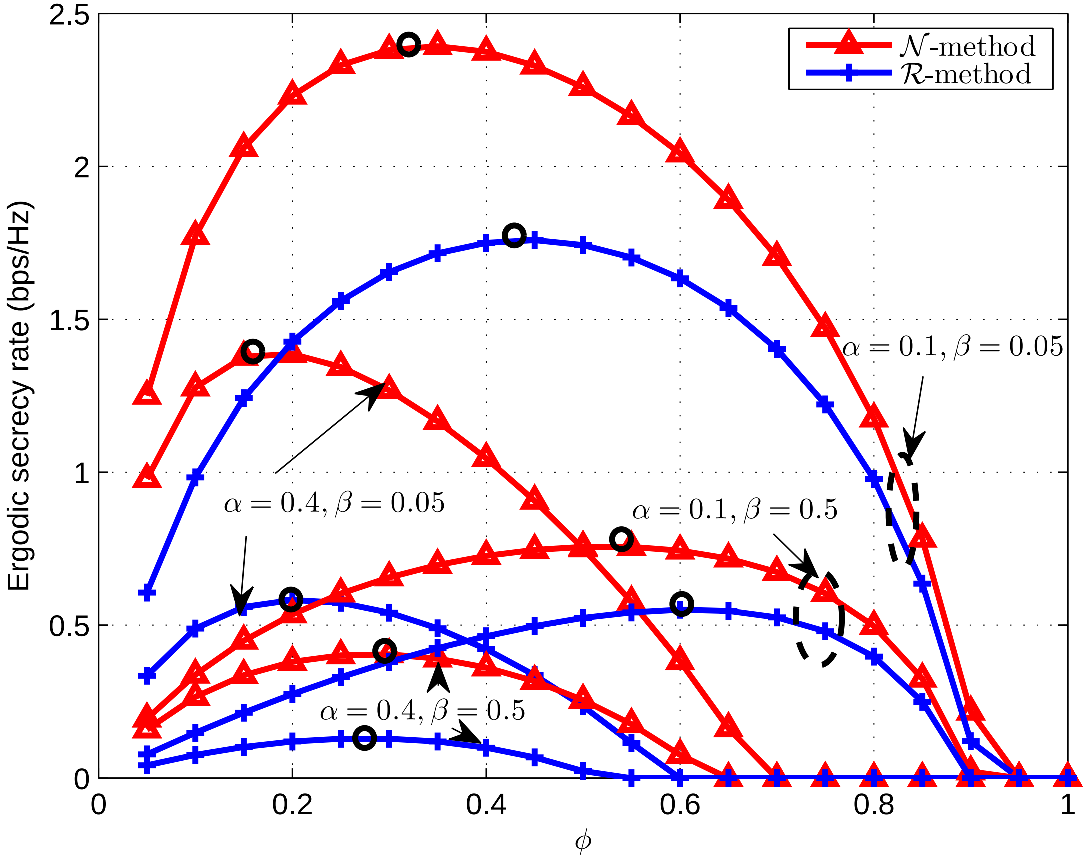

Figure 2.5: Ergodic secrecy rate vs. power allocation factor ϕ assuming perfect training, $N_T = 100$, $M = 7$, $P_T = 10$ dB, and $\rho = 0.1$. Black circles denote the optimal power allocation factor, ϕ^*, obtained with (2.33) and (2.34).

pilot contamination, respectively. We observe that, unlike the case when ϕ is fixed, if ϕ is optimized, the ergodic secrecy rate is a non-increasing function of β also in case of pilot contamination, i.e., for a given number of users, increasing the number of BS antennas is always beneficial. On the other hand, for all considered cases, the optimal value of ϕ is a monotonically increasing function of β, i.e., as the number of users in the system increases relative to the number of BS antennas, less power is allocated to AN. Also, the performance gap between both AN precoding matrix design methods decreases with increasing β.

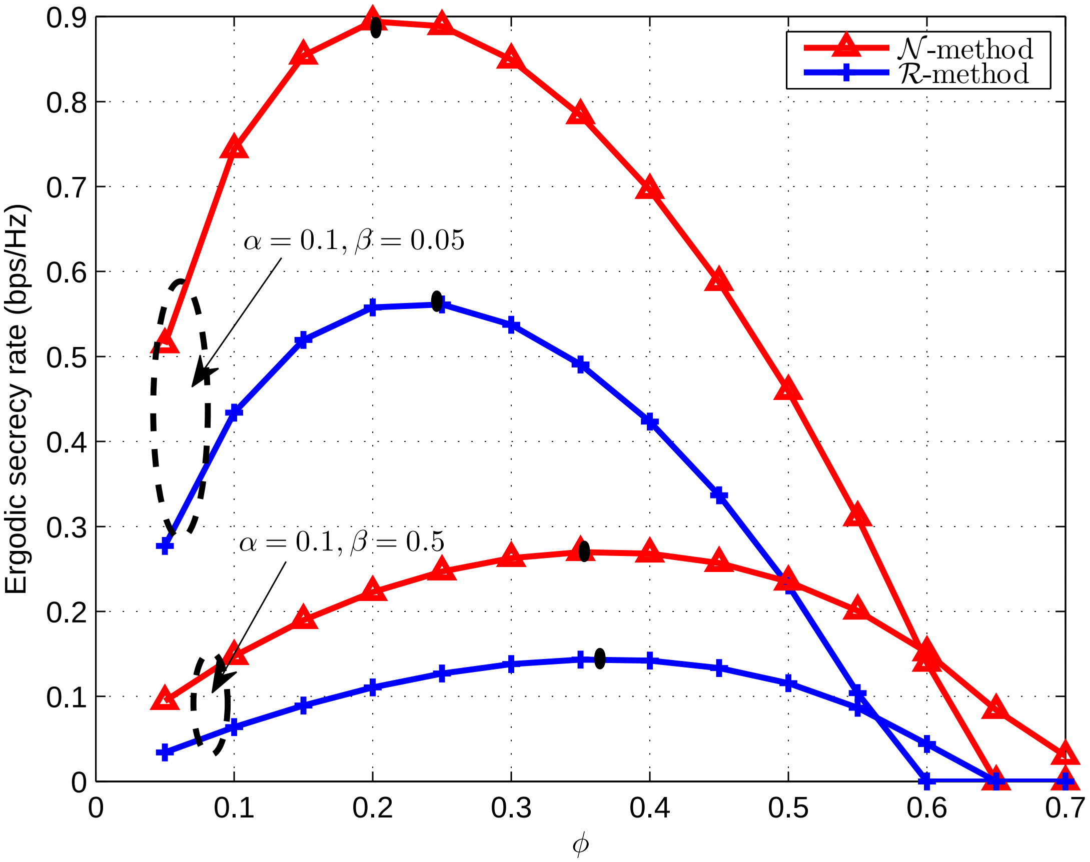

Figure 2.6: Ergodic secrecy rate vs. power allocation factor ϕ assuming pilot contamination, $M = 7$, $N_T = 100$, $P_T = 20$ dB, $\tau = K$, $p_\tau = P_T/K$, and $\rho = 0.1$. Black circles denote the optimal power allocation factor, ϕ^*, obtained with (2.51) and (2.52).

2.6.3 Conditions for Non-zero Ergodic Secrecy Rate

In Fig. 2.8, we illustrate for both AN precoding matrix designs under what conditions a non-zero ergodic secrecy rate is possible. To this end, we plot α_{sec} as defined in (2.29), (2.30), (2.47), and (2.48) as functions of β for $p_\tau = P_T/K$ (subfigure on left hand side) and the amount of power, p_τ, spent by the MTs for training for $\beta = 0.05, 0.5$ (subfigure on right hand side). For $\alpha \geq \alpha_{\text{sec}}$, the ergodic secrecy rate is zero regardless of the amount of power allocated to AN. On the other hand, for

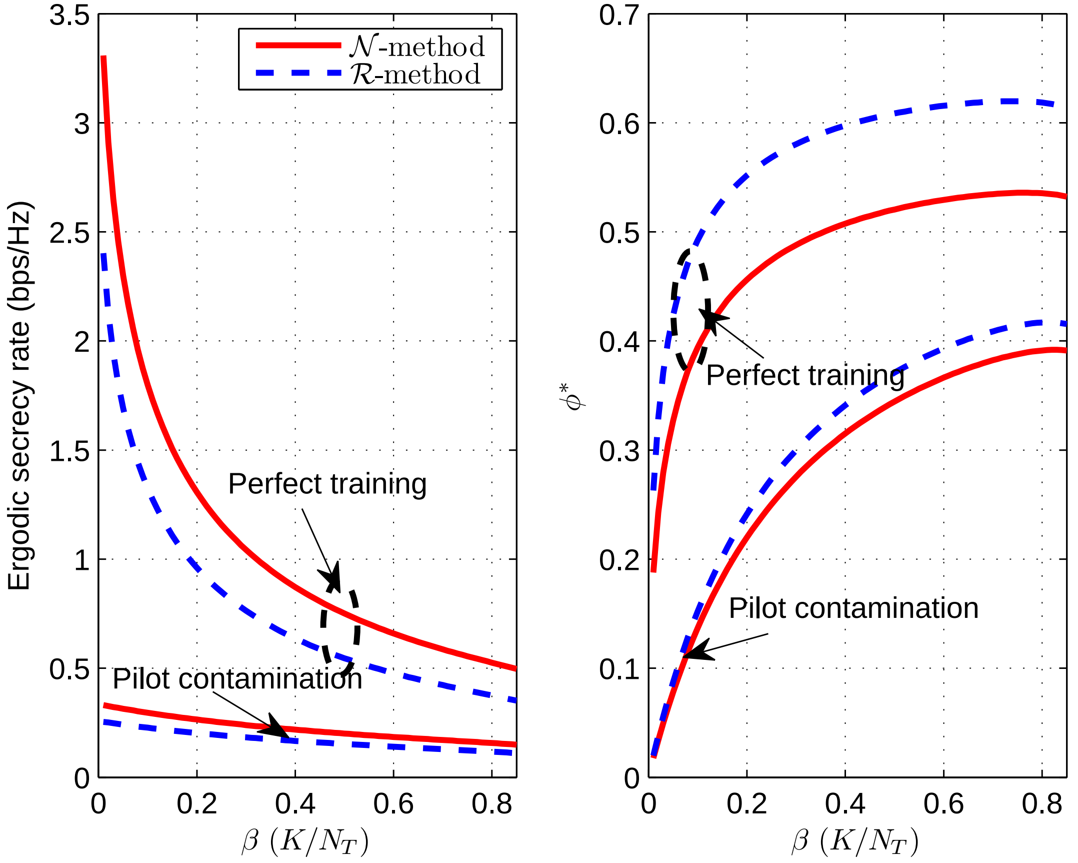

Figure 2.7: Ergodic secrecy rate and optimal power allocation factor, ϕ^*, vs. β for $M = 7$, $P_T = 20$ dB, $N_T = 100$, $\alpha = 0.3$, and $\rho = 0.1$. In case of pilot contamination, $\tau = K$ and $p_\tau = P_T/K$. The ergodic secrecy rates were obtained with (2.27), (2.28), (2.45), and (2.46). The optimal power allocation factor was obtained with (2.33), (2.34), (2.51), and (2.52).

$\alpha < \alpha_{\text{sec}}$, a positive ergodic secrecy rate can be achieved. We observe from Fig. 2.8 that for both AN precoding matrix designs α_{sec} is a decreasing function of β, whereas it is an increasing function of p_τ, i.e., the more reliable the channel estimates, the more eavesdropper antennas can be tolerated before the ergodic secrecy rate drops to zero. However, α_{sec} saturates for large values of p_τ. We note that the values of α_{sec} are smaller for the $\mathcal{R}$-method than for the $\mathcal{N}$-method because of the larger intra-cell

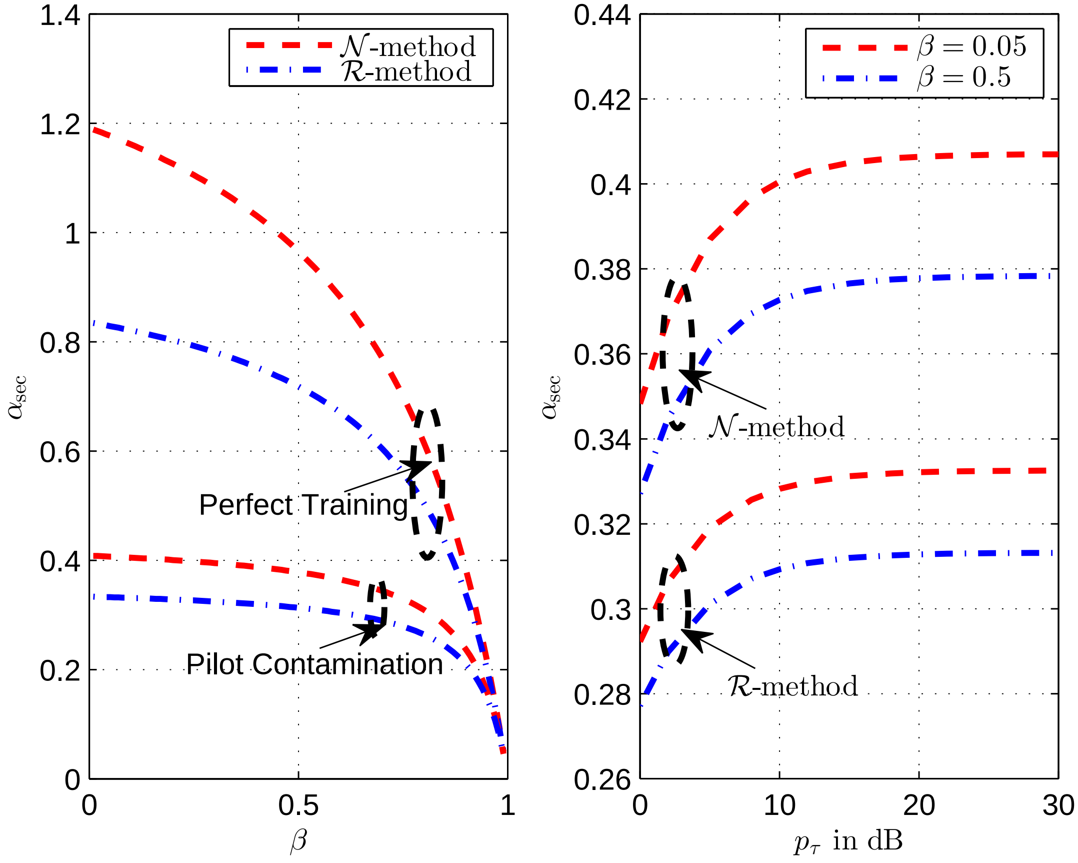

Figure 2.8: $\alpha_{\rm sec}$ vs. β and p_τ for pilot contamination, total transmit power $P_T = 20$ dB, $M = 7$, $N_T = 100$, $\rho = 0.1$, and $\tau = K$.

AN leakage caused by the $\mathcal{R}$-method.

2.6.4 Optimization of the Net Ergodic Secrecy Rate

Fig. 2.9 depicts the net ergodic secrecy rate, $(1-\tau/T)R_{nk}^{\rm sec}$, as a function of λ, where the lower bounds in (2.45) and (2.46) were used to approximate $R_{nk}^{\rm sec}$. The cases of $T = 100$ and $T = 500$ are considered for $K = 5$ and $K = 20$ MTs. We assume that $p_\tau = 0$ dB and λ is varied by changing τ and the optimal power allocation factor ϕ^* is employed. Thereby, the range of possible τ is $[K, T)$, which directly translates into

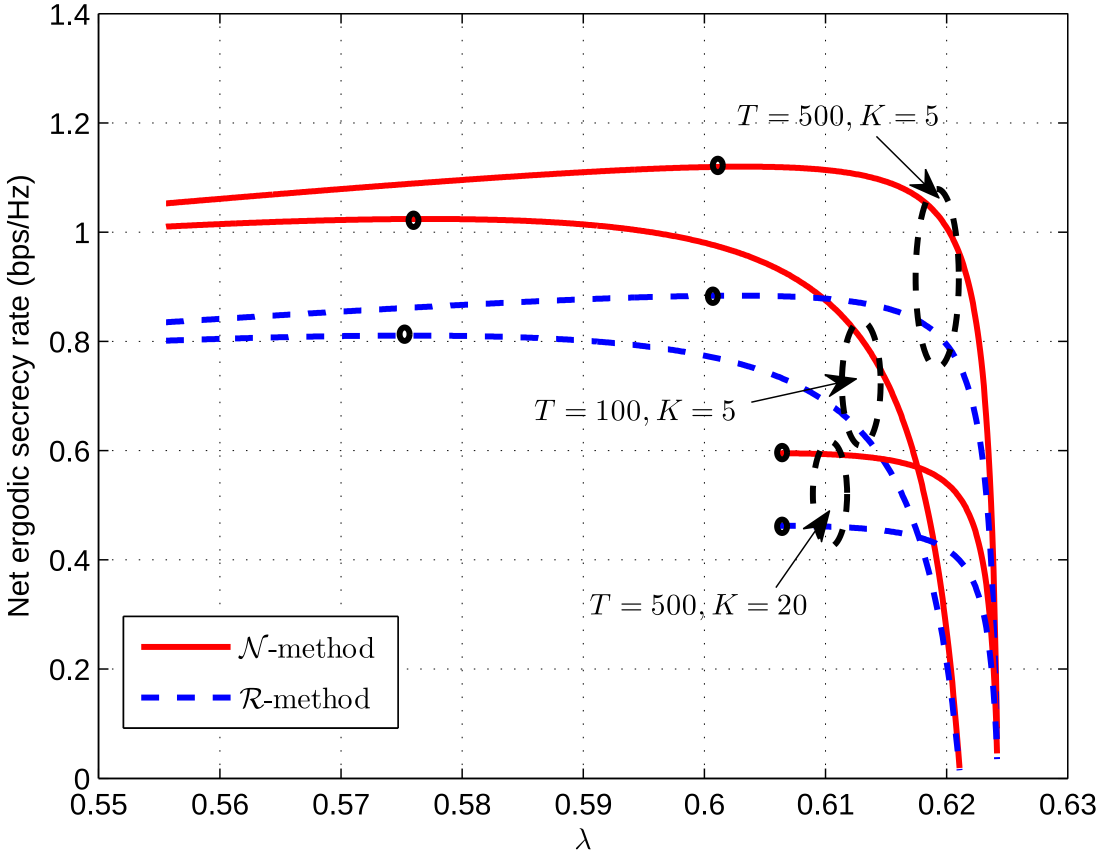

Figure 2.9: Net ergodic secrecy rate vs. λ for a system with optimal ϕ^*, $N_T = 100$, $M = 7$, $\alpha = 0.1$, $P_T = 10$ dB, $p_\tau = 0$ dB, and $\rho = 0.1$. Black circles denote the maximum net ergodic secrecy rate.

the range of possible λ as $\lambda = \frac{p_\tau \tau}{1+p_\tau \tau a}$. Fig. 2.9 reveals that the optimal λ is (slightly) increasing in T since for larger values of T, more time for allocation to uplink training is available, i.e., τ can be increased resulting in a larger value for the optimal λ. For $K = 20$, the lower limit of the permissible interval for τ given by $\tau = K$ yields the maximum net secrecy rate. In this case, increasing τ beyond $\tau = K$ does not improve R_{nk}^{sec} sufficiently to compensate for the decrease of the term $1 - \tau/T$.

2.7 Conclusions

In this chapter, we considered a multi-cell massive MIMO system with MF precoding and AN precoding at the BS for secure downlink transmission in the presence of a multi-antenna passive eavesdropper. For AN precoding, we considered both the conventional NS AN precoding matrix design and a novel random AN precoding matrix design. For both perfect training and pilot contamination, we derived two tight lower bounds on the ergodic secrecy rate and a tight upper bound on the secrecy outage probability. The analytical expressions allowed us to optimize the amount of power allocated to AN precoding and to gain significant insight into the impact of the system parameters on performance. In particular, our results reveal that for the considered multi-cell massive MIMO system with MF precoding (1) AN precoding is necessary to achieve a non-zero ergodic secrecy rate if the user and the eavesdropper experience the same path-loss, (2) secrecy cannot be guaranteed if the eavesdropper has too many antennas, (3) for the case of pilot contamination, the ergodic secrecy rate is only an increasing function of the number of BS antennas if the amount of power allocated to AN precoding is optimized, and (4) the proposed random AN precoding matrix design is a promising low-complexity alternative to the conventional NS AN precoding matrix design.

Chapter 3

Linear Data and AN Precoding in Secure Massive MIMO Systems

3.1 Introduction

Since secrecy and privacy are critical concerns for the design of future communication systems [10], it is of interest to investigate how the large number of spatial degrees of freedom in massive MIMO systems can be exploited for secrecy enhancement [27, 30]. If the eavesdropper (Eve) remains passive to hide its existence, neither the transmitter (Alice) nor the legitimate receiver (Bob) will be able to learn Eve's CSI. In this situation, it is advantageous to inject AN at the transmitter to degrade Eve's channel and to use linear precoding to avoid impairment to Bob's channel as was shown in [24, 27]-[38] and [70], for single user and single-cell multiuser systems, respectively. However, in multi-cell massive MIMO systems, multi-cell interference and pilot contamination will hamper Alice's ability to degrade Eve's channel and to protect Bob's channel. This problem was studied first in Chapter 2 for simple MF data precoding and NS and random AN precoding. However, it is well known that MF data precoding suffers from a large loss in the achievable information rate compared to other linear data precoders such as ZF and RCI precoders as the number of MTs increases [7]. Since it is expected that this loss in information rate also translates into a loss in secrecy rate, studying the secrecy performance of ZF and RCI data precoders in massive MIMO systems is of interest. Furthermore, while NS AN precoding was shown to achieve a better performance compared to random AN precoding [43], it also entails a much higher complexity. Similarly, the improved performance of ZF and RCI data precoding compared to MF data precoding comes at the expense of a higher complexity. Hence, the design of novel data and AN precoders which allow a flexible tradeoff between complexity and secrecy performance is desirable. In the literature, ZF and RCI data precoding were analyzed in the large system limit in [14, 15]. However, neither pilot contamination nor AN were taken into account and the secrecy rate was not analyzed. Using a concept that was originally conceived for CDMA uplink systems in [16] and later extended to MIMO systems in [17], reduced complexity linear data precoders that are based on matrix polynomials were investigated for use in massive MIMO systems in [72, 73]. However, [72, 73] did not take into account the effect of AN leakage for precoder design and did not study the secrecy rate. Hence, the results presented in [72, 73], as well as the related work discussed in Chapter 1.3 [47]-[59], are not directly applicable to the system studied in this chapter.

In this chapter, we consider secure downlink transmission in a multi-cell massive MIMO system employing linear data and AN precoding in the presence of a passive multi-antenna eavesdropper. We study the achievable ergodic secrecy rate of such systems for different linear precoding schemes taking into account the effects of uplink channel estimation, pilot contamination, multi-cell interference, and path-loss. The main contributions of this chapter are summarized as follows:

- To address the impairments incurred by inter-cell interference as well as inter-cell AN leakage, we study both selfish and collaborative precoders. The former requires only the CSI of the MTs in the local cell but cause inter-cell interference and inter-cell AN leakage, whereas the latter requires the CSI between the local BS and the MTs in all cells, but reduce inter-cell interference and inter-cell AN leakage. Nevertheless, since the additional CSI required for the collaborative precoders can be estimated directly by the local BS, the additional overhead and complexity incurred compared to selfish precoders is limited.

- We derive novel closed-form expressions for the asymptotic ergodic secrecy rate which facilitate the performance comparison of different combinations of linear data precoders (i.e., MF, selfish and collaborative ZF/RCI) and AN precoders (i.e., random, selfish and collaborative NS), and provide significant insight for system design and optimization.

- In order to avoid the computational complexity and potential stability issues in fixed point implementations entailed by the large-scale matrix inversions required for ZF and RCI data precoding and NS AN precoding, we propose POLY data and AN precoders and optimize their coefficients. Unlike [71] and [72], which considered polynomial data precoders for massive MIMO systems without AN generation, we use free probability theory [61] to obtain the POLY coefficients, which allows us to express the coefficients as simple functions of the channel and system parameters. Simulation results reveal that these precoders are able to closely approach the performance of selfish RCI data and NS AN precoders, respectively.

The remainder of this chapter is organized as follows. In Section 3.2, we outline the considered system model and review some basic results from Chapter 2. In Sections 3.3 and 3.4, the considered linear data and AN precoders are investigated, respectively. In Section 3.5, the ergodic secrecy rates of different linear precoders are compared analytically for a simple path-loss model. Simulation and numerical results are presented in Section 3.6, and some conclusions are drawn in Section 3.7.

3.2 System Model and Preliminaries

In this section, we introduce the considered system model as well as the adopted channel estimation scheme, and review some ergodic secrecy rate results.

3.2.1 System Model

We consider the downlink of a multi-cell massive MIMO system with cell set $\mathcal{M} = \{1, \dots, M\}$ and a frequency reuse factor of one, i.e., all BSs use the same spectrum. Each cell includes one N_T-antenna BS, $K \leq N_T$ single-antenna MTs, and potentially an N_E-antenna eavesdropper. The eavesdroppers try to hide their existence and hence remain passive. As a result, the BSs cannot estimate the eavesdroppers' CSI. To overcome this limitation, each BS generates AN to mask its information-carrying signal and to prevent eavesdropping [24]. In the following, the k^{th} MT, $k = 1, \dots, K$, in the n^{th} cell, $n = 1, \dots, M$, is the MT of interest and we assume that an eavesdropper tries to decode the signal intended for this MT. We note that neither the BSs nor the MTs are assumed to know which MT is targeted by the eavesdropper. The signal vector, $\mathbf{x}_n \in \mathbb{C}^{N_T \times 1}$, transmitted by the BS in the n^{th} cell (also referred to as the n^{th} BS in the following) is given by

$$\mathbf{x}_n = \sqrt{p}\mathbf{F}_n\mathbf{s}_n + \sqrt{q}\mathbf{A}_n\mathbf{z}_n, \tag{3.1}$$

where $\mathbf{s}_n \sim \mathbb{CN}(\mathbf{0}_K, \mathbf{I}_K)$ and $\mathbf{z}_n \sim \mathbb{CN}(\mathbf{0}_{N_T}, \mathbf{I}_{N_T})$ denote the data and AN vectors for the K MTs in the n^{th} cell, respectively. $\mathbf{F}_n = [\mathbf{f}_{n1}, \cdots, \mathbf{f}_{nK}] \in \mathbb{C}^{N_T \times K}$ and

$\mathbf{A}_n = [\mathbf{a}_{n1}, \cdots, \mathbf{a}_{nN_T}] \in \mathbb{C}^{N_T \times N_T}$ are the data and AN precoding matrices, respectively, and the efficient design of these matrices is the main scope of this chapter. Thereby, the structure of both types of precoding matrices does not depend on which MT is targeted by the eavesdropper. The AN precoding matrix $\mathbf{A}_n$ has rank $L = \text{rank}\{\mathbf{A}_n\} \leq N_T$, i.e., L dimensions of the N_T-dimensional signal space spanned by the N_T BS antennas are exploited for jamming of the eavesdropper. The data and AN precoding matrices are normalized as $\text{tr}\{\mathbf{F}_n^H \mathbf{F}_n\} = K$ and $\text{tr}\{\mathbf{A}_n^H \mathbf{A}_n\} = L$, i.e., their average power per dimension is one. The average powers p and q allocated to the information-carrying signal for each MT and each AN signal, respectively, can be written as $p = \frac{\phi P_T}{K}$ and $q = \frac{(1-\phi)P_T}{L}$, where P_T is the total transmit power and $\phi \in (0, 1]$ is a power allocation factor which can be optimized. For the sake of clarity, in this chapter, we assume that all cells utilize the same value of ϕ.

The vectors collecting the received signals at the K MTs and the N_E antennas of the eavesdropper in the n^{th} cell are given by

$$\mathbf{y}_n = \sum_{m=1}^{M} \mathbf{G}_{mn} \mathbf{x}_m + \mathbf{n}_n \qquad \text{and} \qquad \mathbf{y}_E = \sum_{m=1}^{M} \mathbf{G}_{mE} \mathbf{x}_m + \mathbf{n}_E, \tag{3.2}$$

respectively, with Gaussian noise vectors $\mathbf{n}_n \in \mathbb{CN}(\mathbf{0}_K, \sigma_n^2 \mathbf{I}_K)$ and $\mathbf{n}_E \in \mathbb{CN}(\mathbf{0}_{N_E}, \sigma_E^2 \mathbf{I}_{N_E})$, where σ_n^2 and σ_E^2 denote the noise variances at one MT and one eavesdropper receive antenna, respectively. Furthermore, $\mathbf{G}_{mn} = \mathbf{D}_{mn}^{1/2} \mathbf{H}_{mn} \in \mathbb{C}^{K \times N_T}$ and $\mathbf{G}_{mE} = \sqrt{\beta_{mE}} \mathbf{H}_{mE} \in \mathbb{C}^{N_E \times N_T}$ are the matrices modeling the channels from the m^{th} BS to the K MTs and the eavesdropper in the n^{th} cell, respectively. Thereby, $\mathbf{D}_{mn} = \text{diag}\{\beta_{mn}^1, \ldots, \beta_{mn}^K\}$ and β_{mE} represent the path-losses from the m^{th} BS to the K MTs and the eavesdropper in the n^{th} cell, respectively. Matrix $\mathbf{H}_{mn} \in \mathbb{C}^{K \times N_T}$, with row vector $\mathbf{h}_{mn}^k \in \mathbb{C}^{1 \times N_T}$ in the k^{th} row, and matrix $\mathbf{H}_{mE} \in \mathbb{C}^{N_E \times N_T}$ represent the corresponding small-scale fading components. Their elements are modeled as mutually independent and identically distributed (i.i.d.) complex Gaussian random variables (r.v.s) with zero mean and unit variance.

For the design of the data and noise precoders, we consider two different approaches: *Selfish* designs and *collaborative* designs. For the selfish designs, each BS designs its precoders only based on the estimate of the CSI in its own cell, $\mathbf{G}_{nn}$, and without regard for the interference and the AN it causes to other cells. In contrast, for the collaborative designs, each BS designs its precoders based on the estimates of the CSI to the MTs in all cells, $\mathbf{G}_{mn}$, $m = 1, \ldots, M$, in an effort to avoid excessive interference and AN to other cells. Although collaborative designs introduce more channel estimation overhead at the BS, they may not always outperform selfish designs because of the imperfection of the CSI and the limited number of spatial degrees of freedom available for precoder design.

3.2.2 Channel Estimation and Pilot Contamination

As is customary for massive MIMO systems, we assume that the downlink and uplink channels are reciprocal and the CSI is estimated in an uplink training phase [2]-[8]. To this end, all MTs emit pilot sequences of length $\tau = \xi K, \xi \in \mathcal{M}$ and with pilot symbol power p_τ. We assume that the pilot sequences are mutually orthogonal, and thus can be assigned to at most ξ cells without mutual pollution. When $\xi < M$, this gives rise to so-called pilot contamination [2]-[8], because at least one pilot sequence is shared between more than one MTs in a M-cell network. Furthermore, we assume that the path-loss information changes on a much slower time scale than the small-scale fading. Hence, the path-loss matrices $\mathbf{D}_{nm}$, $m = 1, \ldots, M$, can be estimated perfectly and are assumed to be known at the BS for MMSE estimation of the small-scale fading gains [8]. At the n^{th} BS, the estimate of the small-scale fading vector to the k^{th} MT in the m^{th} cell, $\hat{\mathbf{h}}_{nm}^{k}$, is obtained in Appendix B.1. For MMSE estimation, we have

$$\mathbf{h}_{nm}^{k} = \hat{\mathbf{h}}_{nm}^{k} + \tilde{\mathbf{h}}_{nm}^{k}, \tag{3.3}$$

where the estimate $\hat{\mathbf{h}}_{nm}^{k}$ and the estimation error $\tilde{\mathbf{h}}_{nm}^{k}$ are mutually independent and can be statistically characterized as $\hat{\mathbf{h}}_{nm}^{k} \sim \mathbb{CN}(\mathbf{0}_{N_T}, \frac{p_\tau \tau \beta_{nm}^{k}}{\theta_{nm}^{k} + p_\tau \tau \beta_{nm}^{k}} \mathbf{I}_{N_T})$ and $\tilde{\mathbf{h}}_{nm}^{k} \sim \mathbb{CN}(\mathbf{0}_{N_T}, \frac{\theta_{nm}^{k}}{\theta_{nm}^{k} + p_\tau \tau \beta_{nm}^{k}} \mathbf{I}_{N_T})$, respectively, cf. [43], where $\theta_{nm}^{k} = 1 + p_\tau \tau \sum_{l \in \mathcal{M}_m \subseteq \mathcal{M} \setminus \{m\}} \beta_{nl}^{k}$ and $\mathcal{M}_m$ denotes the set of cells sharing the same set of pilot sequences with the m^{th} cell, which is a subset of $\mathcal{M}$ excluding the m^{th} cell, where

$$\lfloor M/\xi \rfloor - 1 \leq |\mathcal{M}_m| \leq \lceil M/\xi \rceil - 1, \forall m. \tag{3.4}$$

Example: For $M = 7$, $\xi = 2$, we have $2 \leq |\mathcal{M}_m| \leq 3$, i.e., there are 2 or 3 cells sharing the same set of pilot sequences with the m^{th} cell [5].

To further clarify, when $\xi = M$, i.e., all MK MTs use their respective pilots, no pilot contamination exists, θ_{nm}^{k} reduces to 1 as $|\mathcal{M}_m| = 0$ in this case. For $\xi = 1$, i.e., the pilot sequences in one cell are orthogonal, but reused in all other cells, we simply have $|\mathcal{M}_m| = M - 1$, and the distributions of both $\hat{\mathbf{h}}_{nm}^{k}$ and $\tilde{\mathbf{h}}_{nm}^{k}$ are identical with those in Chapter 2. For future reference, we collect the estimates and the estimation errors at the n^{th} BS corresponding to all K MTs in the m^{th} cell in matrices $\hat{\mathbf{H}}_{nm} = [(\hat{\mathbf{h}}_{nm}^{1})^T, \ldots, (\hat{\mathbf{h}}_{nm}^{K})^T]^T \in \mathbb{C}^{K \times N_T}$ and $\tilde{\mathbf{H}}_{nm} = [(\tilde{\mathbf{h}}_{nm}^{1})^T, \ldots, (\tilde{\mathbf{h}}_{nm}^{K})^T]^T \in \mathbb{C}^{K \times N_T}$, respectively.

[5] For the results shown in Section 3.6, without loss of generality, we always assume $|\mathcal{M}_n| = 3$ for calculating the secrecy rate achieved by the MT in the n^{th} cell when the parameters in this example are adopted.

3.2.3 Ergodic Secrecy Rate

The performance metric adopted in this chapter is the ergodic secrecy rate [30]. In this section, we review some results for the ergodic secrecy rate in multi-cell massive MIMO systems employing linear data and AN precoding from [43], as these results will be needed throughout this chapter. Combining (3.1) and (3.2) we observe that the downlink channel comprising the BS, the k^{th} MT, and the eavesdropper in the n^{th} cell is an instance of a MISOME wiretap channel [27]. Hence, the achievable secrecy rate of the k^{th} MT in the n^{th} cell is bounded by the difference of the capacities of the channel between the BS and the MT and the channel between the BS and the eavesdropper, see [43, Lemma 1], [47, Lemma 2]. Thus, a lower bound on the ergodic secrecy rate of the k^{th} MT in the n^{th} cell is given by [43]

$$R_{nk}^{\text{sec}} = [R_{nk} - C_{nk}^{\text{eve}}]^{+}, k = 1, \ldots, K, \tag{3.5}$$

where R_{nk} denotes an achievable rate of the k^{th} MT in the n^{th} cell and C_{nk}^{eve} denotes the ergodic capacity of the channel between the BS and the eavesdropper. In order to obtain a tractable lower bound on the ergodic secrecy rate, we lower bound the achievable rate of the MT as $R_{nk} = \log_2(1 + \gamma_{nk})$ with SINR [43, Eq. (10)] $\gamma_{nk} =$

$$\frac{|\mathbb{E}[\sqrt{\beta_{nn}^{k} p}\mathbf{h}_{nn}^{k}\mathbf{f}_{nk}]|^2}{\text{var}[\sqrt{\beta_{nn}^{k} p}\mathbf{h}_{nn}^{k}\mathbf{f}_{nk}] + \sum\limits_{m=1}^{M}\sum\limits_{i=1}^{N_t}\mathbb{E}[|\sqrt{\beta_{mn}^{k} q}\mathbf{h}_{mn}^{k}\mathbf{a}_{mi}|^2] + \sum\limits_{\{m,l\}\neq\{n,k\}}\mathbb{E}[|\sqrt{\beta_{mn}^{k} p}\mathbf{h}_{mn}^{k}\mathbf{f}_{ml}|^2] + 1}. \tag{3.6}$$

Furthermore, we make the pessimistic assumption that the eavesdropper is able to cancel the received signals of all in-cell and out-of-cell MTs except the signal intended for the MT of interest. This leads to an upper bound for the eavesdropper's capacity, and consequently, to a lower bound for the ergodic secrecy rate.[6] Hence, the ergodic capacity of the eavesdropper is given by [43, Eq. (7)]

$$C_{nk}^{\mathrm{eve}} = \mathbb{E}\left[\log_2 \left(1 + p\mathbf{f}_{nk}^H \mathbf{G}_{nE}^H \mathbf{X}^{-1} \mathbf{G}_{nE} \mathbf{f}_{nk}\right) \right], \tag{3.7}$$

where $\mathbf{X} = q\sum_{m=1}^{M} \mathbf{G}_{mE}\mathbf{A}_m\mathbf{A}_m^H\mathbf{G}_{mE}^H \in \mathbb{C}^{N_T \times N_T}$ denotes the noise correlation matrix at the eavesdropper under the worst-case assumption that the receiver noise at the eavesdropper is negligible, i.e., $\sigma_E^2 \to 0$. Denoting the normalized number of eavesdropper antennas by $\alpha = N_E/N_T$, a necessary condition for the invertibility of matrix $\mathbf{X}$ is $\alpha \leq ML/N_T$. Hence, a non-zero secrecy rate can only be achieved if this condition is met. Consequently, a larger L implies that the BS is able to tolerate more eavesdropper antennas.

If $\mathbf{H}_{nE}\mathbf{f}_{nk}$ and matrix $\mathbf{X}$ are statistically independent, which in turn means for the data and AN precoders that vector $\mathbf{f}_{nk}$ and the subspace spanned by the columns of $\mathbf{A}_n$ are mutually orthogonal, a simple and tight upper bound on (3.7) can be obtained. Since any efficient data/AN precoder pair has to keep the AN self-interference at the desired MT small, this orthogonality condition holds at least approximately in practice. In this case, for $\alpha < a^2L/(cN_T)$ and $N_T \to \infty$, where $a = 1 + \sum_{m\neq n}^{M} \beta_{mE}/\beta_{nE}$ and $c = 1 + \sum_{m\neq n}^{M} (\beta_{mE}/\beta_{nE})^2$, a simple and tight upper bound for C_{nk}^{eve} is given by [43, Theorem 1]

$$C_{nk}^{\mathrm{eve}} \leq \log_2\left(1 + \frac{\alpha p}{aqL/N_T - c\alpha q/a}\right) = \log_2\left(1 + \frac{\alpha\phi}{\beta(1-\phi)(a - c\alpha N_T/(La))}\right). \tag{3.8}$$

For $M = 1$, we have $a^2/c = M = 1$, i.e., the bound in (3.8) is applicable in the

[6] This lower bound is achievable if the eavesdropper has access to the data of all interfering in-cell and out-of-cell MTs, which might be the case e.g. if the interfering MTs cooperate with the eavesdropper.

entire range of α where C_{nk}^{eve} in (3.7) is finite. For $M > 1$, we have $a^2/c \leq M$, i.e., the bound is not applicable for $La^2/(cN_T) \leq \alpha \leq ML/N_T$. However, for strong inter-cell interference, we have $\beta_{mE} \approx \beta_{nE}$ and $a^2/c \approx M$, i.e., the bound is applicable for all α for which C_{nk}^{eve} in (3.7) is finite. On the other hand, for weak inter-cell interference, we have $\beta_{mE} \ll \beta_{nE}$, and matrix $\mathbf{X}$ will be ill-conditioned for $L/N_T \leq \alpha \leq ML/N_T$ and C_{nk}^{eve} will become very large. Hence, the bound is again applicable for the values of α (i.e., $0 \leq \alpha \leq L/N_T$), for which C_{nk}^{eve} in (3.7) assumes practically relevant values. More generally, [43, Figs. 2-4] and Section 3.6 suggest that (3.8) is applicable and tight for all values of α which permit a non-vanishing secrecy rate.

Combining (3.5), (3.6), and (3.8), we obtain a tight and tractable lower bound on the secrecy rate [43]. It is noteworthy that the upper bound on the capacity of the eavesdropper in (3.8) is only affected by the dimensionality of the AN precoder, L, but not on the exact structures of $\mathbf{A}_n$ and $\mathbf{F}_n$, as long as $\mathbf{f}_{nk}$ and the subspace spanned by the columns of $\mathbf{A}_n$ are orthogonal. On the other hand, the achievable rate of the MT in (3.6) is affected by both the data and the AN precoders. In the following two sections, we analyze the impact of the most important existing data and AN precoder designs on the achievable rate R_{nk} as $N_T \to \infty$, respectively, and propose novel low-complexity data and AN precoders that are based on a polynomial matrix expansion.

3.3 Linear Data Precoders for Secure Massive MIMO

In this section, we analyze the achievable rate of selfish and collaborative ZF/RCI data precoding, respectively, and develop a novel POLY data precoder. In contrast to existing analysis and designs of data precoders for massive MIMO, e.g. [14, 15], [72, 73], the results presented in this section account for the effect of AN leakage, which is only present if AN is injected at the BS for secrecy enhancement. We are interested in the asymptotic regime where $K, N_T \to \infty$ but $\beta = K/N_T$ and $\alpha = N_E/N_T$ are finite.

3.3.1 Analysis of Existing Data Precoders

For $N_T \to \infty$, analyzing the achievable rate is equivalent to analyzing the SINR in (3.6). Thereby, the effect of the AN precoder can be captured by the term

$$Q = \sum_{m=1}^{M} \sum_{i=1}^{N_t} \mathbb{E}[|\sqrt{\beta_{mn}^{k}} \mathbf{h}_{mn}^{k} \mathbf{a}_{mi}|^2] = \sum_{m=1}^{M} \beta_{mn}^{k} \mathbb{E}[\mathbf{h}_{mn}^{k} \mathbf{A}_m \mathbf{A}_m^H (\mathbf{h}_{mn}^{k})^H] \tag{3.9}$$

in the denominator of (3.6), which represents the inter-cell and intra-cell AN leakage. This term is assumed to be given in this section and will be analyzed in detail for different AN precoders in Section 3.4.

Selfish ZF/RCI Data Precoding

The selfish RCI (SRCI) data precoder for the n^{th} cell is given by

$$\mathbf{F}_n = \gamma_1 \mathbf{L}_{nn} \hat{\mathbf{H}}_{nn}^H, \tag{3.10}$$

where $\mathbf{L}_{nn} = (\hat{\mathbf{H}}_{nn}^H \hat{\mathbf{H}}_{nn} + \kappa_1 \mathbf{I}_{N_T})^{-1}$, γ_1 is a scalar normalization constant, and κ_1 is a regularization constant. In the following proposition, we provide the resulting SINR of the k^{th} MT in the n^{th} cell.

Proposition 3.1. *For SRCI data precoding, the received SINR at the k^{th} MT in the*

n^{th} cell is given by

$$\gamma_{nk}^{\text{SRCI}} = \frac{1}{\frac{\sum_{m\in\mathcal{M}_n\cup\{n\}}\hat{\Gamma}_{\text{SRCI}}^{m}+(1+\mathcal{G}(\beta,\kappa_1))^2}{\mathcal{G}(\beta,\kappa_1)\left(\hat{\Gamma}_{\text{SRCI}}^{n}+\frac{\hat{\Gamma}_{\text{SRCI}}^{n}\kappa_1}{\beta}(1+\mathcal{G}(\beta,\kappa_1))^2\right)}+\sum_{m\in\mathcal{M}_n}\lambda_{mk}/\lambda_{nk}}, \tag{3.11}$$

where the set $\mathcal{M}_n$ is defined in Section 3.2,

$$\mathcal{G}(\beta,\kappa_1) = \frac{1}{2}\left[\sqrt{\frac{(1-\beta)^2}{\kappa_1^2}+\frac{2(1+\beta)}{\kappa_1}+1}+\frac{1-\beta}{\kappa_1}-1\right], \tag{3.12}$$

and

$$\hat{\Gamma}_{\text{SRCI}}^{m} = \frac{\Gamma_{\text{SRCI}}\lambda_{mk}}{\Gamma_{\text{SRCI}}\sum_{m\in\mathcal{M}_n\cup\{n\}}\mu_{mk}+1} \tag{3.13}$$

with

$$\Gamma_{\text{SRCI}} = \frac{K}{\sum_{m\notin\mathcal{M}_n\bigcup\{n\}}\sum_{l=1}^{K}\beta_{mn}^{k}+\eta Q+\frac{K}{\phi P_T}}, \tag{3.14}$$

$\lambda_{mk} = \beta_{mn}^{k}\frac{p_\tau\tau\beta_{mn}^{k}}{\theta_{mn}^{k}+p_\tau\tau\beta_{mn}^{k}}$, $\mu_{mk} = \beta_{mn}^{k}\frac{\theta_{mn}^{k}}{\theta_{mn}^{k}+p_\tau\tau\beta_{mn}^{k}}$, *and* $\eta = q/p$.

Proof. Please refer to Appendix B.2. □

Regularization constant κ_1 can be optimized for maximization of the lower bound on the secrecy rate in (3.5), which is equivalent to maximizing the SINR in (3.11). Setting the derivative of $\gamma_{nk}^{\text{SRCI}}$ with respect to κ_1 to zero, the optimal regularization parameter is found as $\kappa_{1,\text{opt}} = \beta/\sum_{m\in\mathcal{M}_n\cup\{n\}}\hat{\Gamma}_{\text{SRCI}}^{m}$ in Appendix B.3, and the corresponding maximum SINR is given by

$$\gamma_{nk}^{\text{SRCI}} = \frac{1}{\hat{\Gamma}_{\text{SRCI}}^{n}/\sum_{m\in\mathcal{M}_n\cup\{n\}}\hat{\Gamma}_{\text{SRCI}}^{m}\mathcal{G}(\beta,\kappa_{1,\text{opt}})+\sum_{m\in\mathcal{M}_n}\lambda_{mk}/\lambda_{nk}}. \tag{3.15}$$

On the other hand, for $\kappa_1 \to 0$, the SRCI data precoder in (3.10) reduces to the selfish ZF (SZF) data precoder. The corresponding received SINR is provided in the following corollary.

Corollory 3.1. *Assuming $\beta < 1$, for SZF data precoding, the received SINR at the k^{th} MT in the n^{th} cell is given by*

$$\gamma_{nk}^{\text{SZF}} = \frac{1}{\frac{\beta}{(1-\beta)\hat{\Gamma}_{\text{SRCI}}} + \sum_{m\in\mathcal{M}_n} \lambda_{mk}/\lambda_{nk}}. \tag{3.16}$$

Proof. Please refer to Appendix B.4. □

Collaborative ZF/RCI Precoding

The collaborative RCI (CRCI) precoder for the n^{th} cell is given by

$$\mathbf{F}_n = \gamma_2 \mathbf{L}_n \hat{\mathbf{H}}_{nn}^H, \tag{3.17}$$

where $\mathbf{L}_n = (\hat{\mathbf{H}}_n^H \hat{\mathbf{H}}_n + \kappa_2 \mathbf{I}_{N_T})^{-1}$ with $\hat{\mathbf{H}}_n = [\hat{\mathbf{H}}_{n1}^T \dots \hat{\mathbf{H}}_{nM}^T]^T \in \mathbb{C}^{MK\times N_T}$, γ_2 is a normalization constant, and κ_2 is a regularization constant. The corresponding SINR of the k^{th} MT in the n^{th} cell is provided in the following proposition.

Proposition 3.2. *For CRCI data precoding, the received SINR at the k^{th} MT in the n^{th} cell is given by*

$$\gamma_{nk}^{\text{CRCI}} = \frac{1}{\frac{\sum_{m=1}^{M} \hat{\Gamma}_{\text{CRCI}}^{m} + (1+\mathcal{G}(\xi\beta,\kappa_2))^2}{\mathcal{G}(\xi\beta,\kappa_2)\left(\hat{\Gamma}_{\text{CRCI}}^{n} + \frac{\hat{\Gamma}_{\text{CRCI}}^{n}\kappa_2}{\xi\beta}(1+\mathcal{G}(\xi\beta,\kappa_2))^2\right)} + \sum_{m\in\mathcal{M}_n} \lambda_{mk}/\lambda_{nk}}, \tag{3.18}$$

where $\hat{\Gamma}_{\text{CRCI}}^{m} = \frac{\Gamma_{\text{CRCI}}\lambda_{mk}}{\Gamma_{\text{CRCI}}\sum_{m=1}^{M}\mu_{mk}+1}$ with $\Gamma_{\text{CRCI}} = \frac{K}{\eta Q + \frac{K}{\phi P_T}}$.

Proof. The proof is similar to that for the SINR for the SRCI data precoder given in Appendix B.2. □

Furthermore, the optimal regularization constant maximizing the SINR (and thus the secrecy rate) in (3.18) is obtained as $\kappa_{2,\mathrm{opt}} = \xi\beta / \sum_{m=1}^{M} \hat{\Gamma}^{m}_{\mathrm{CRCI}}$, and the corresponding maximum SINR is given by

$$\gamma_{nk}^{\mathrm{CRCI}} = \frac{1}{\hat{\Gamma}^{n}_{\mathrm{CRCI}} / \sum_{m=1}^{M} \hat{\Gamma}^{m}_{\mathrm{CRCI}} \mathcal{G}(\xi\beta, \kappa_{2,\mathrm{opt}}) + \sum_{m \in \mathcal{M}_n} \lambda_{mk}/\lambda_{nk}}. \tag{3.19}$$

On the other hand, for $\kappa_2 \to 0$, the CRCI precoder in (3.17) reduces to the collaborative ZF (CZF) precoder. The corresponding received SINR is provided in the following corollary.

Corollory 3.2. *Assuming $\beta < 1/M$, for CZF data precoding, the received SINR at the k^{th} MT in the n^{th} cell is given by*

$$\gamma_{nk}^{\mathrm{CZF}} = \frac{1}{\frac{\xi\beta}{(1-\xi\beta)\hat{\Gamma}^{n}_{\mathrm{CRCI}}} + \sum_{m \in \mathcal{M}_n} \lambda_{mk}/\lambda_{nk}}. \tag{3.20}$$

Proof. $\gamma_{nk}^{\mathrm{CZF}}$ in (3.20) is obtained by letting $\kappa_2 \to 0$ in (3.18). The proof is similar to that for the SINR for the SZF data precoder given in Appendix B.4. □

Remark 3.1. *By comparing Propositions 3.1 and 3.2, we observe that $\gamma_{nk}^{\mathrm{SRCI}}$ and $\gamma_{nk}^{\mathrm{CRCI}}$ are identical for $\xi = 1$. In this scenario, the estimate of inter-cell CSI at the BS is nothing but a scaled version of that of the in-cell CSI, cf. Chapter 2, and both schemes are equivalent. Therefore, we will focus more on the scenario of $\xi > 1$ in the sequel.*

Remark 3.2. *Selfish data precoders require estimation of in-cell CSI, i.e., $\hat{\mathbf{H}}_{nn}$, only. In contrast, collaborative data precoders require estimation of both in-cell and inter-cell CSI at the BS, i.e., $\hat{\mathbf{H}}_{n}$. Furthermore, since collaborative data precoders attempt to avoid interference not only to in-cell users but also to out-of-cell users, more BS* *antennas are needed to achieve high performance. This is evident from Corollaries 3.1 and 3.2, which reveal that $N_T > K$ and $N_T > \xi K$ are necessary for SZF and CZF data precoding, respectively. On the other hand, if successful, trying to avoid out-of-cell interference is beneficial for the overall performance. Hence, whether selfish or collaborative precoders are preferable depends on the parameters of the considered system, cf. Sections 3.5 and 3.6.*

3.3.2 POLY Data Precoder

The RCI and ZF data precoders introduced in the previous section achieve a higher performance than simple MF data precoding [43]. However, they require a matrix inversion which entails a high computational complexity for the large values of K and N_T desired in massive MIMO. Hence, in this section, we propose a low-complexity POLY data precoder which avoids the matrix inversion. As the goal is a low-complexity design, we focus on selfish POLY precoders, although the extension to collaborative designs is possible.

The proposed POLY precoder, $\mathbf{F}_n$, for the n^{th} BS can be expressed as

$$\mathbf{F}_n = \frac{1}{\sqrt{N_T}} \hat{\bar{\mathbf{H}}}_{nn}^H \sum_{i=0}^{\mathcal{I}} \mu_i \left(\hat{\bar{\mathbf{H}}}_{nn} \hat{\bar{\mathbf{H}}}_{nn}^H \right)^i, \tag{3.21}$$

where $\hat{\bar{\mathbf{H}}}_{nn} = \frac{1}{\sqrt{N_T}} \hat{\mathbf{H}}_{nn}$, and $\boldsymbol{\mu} = [\mu_0, \dots, \mu_{\mathcal{I}}]^T$ are the real-valued coefficients of the precoder matrix polynomial, which have to be optimized. In the following, we show that, for $K, N_T \to \infty$, the optimum coefficients $\boldsymbol{\mu}$ do not depend on the instantaneous channel estimates but are constant and can be determined by exploiting results from free probability [61] and random matrix theory [93]. To this end, we define the asymptotic average MSE of the users in the n^{th} cell as $\mathrm{mse}_n = \lim_{K \to \infty} \frac{1}{K} \mathbb{E}\left[\|\mathbf{e}_n\|^2 \right]$

with error vector

$$\mathbf{e}_n = \varsigma\mathbf{y}_n - \mathbf{s}_n = \varsigma(\mathbf{G}_{nn}(\sqrt{p}\mathbf{F}_n\mathbf{s}_n + \sqrt{q}\mathbf{A}_n\mathbf{z}_n) + \tilde{\mathbf{n}}_n) - \mathbf{s}_n, \tag{3.22}$$

where $\tilde{\mathbf{n}}_n = \sum_{m\neq n}\mathbf{G}_{mn}\mathbf{x}_m + \mathbf{n}_n$ includes Gaussian noise, inter-cell interference, and inter-cell AN leakage. Furthermore, ς is a normalization constant at the receiver, which does not impact detection performance. The optimal coefficient vector $\boldsymbol{\mu}$ minimizes mse_n for a given power budget ϕP_T for the information-carrying signal, i.e.,

$$\min_{\boldsymbol{\mu},\varsigma} \mathrm{mse}_n \qquad \text{s.t.}: \mathrm{Tr}\{\mathbf{F}_n^H\mathbf{F}_n\} = 1, \tag{3.23}$$

where we use the notation $\mathrm{Tr}\left\{\cdot\right\} = \lim_{K\to\infty}\mathrm{tr}\left\{\cdot\right\}/K$. The optimal coefficient vector, $\boldsymbol{\mu}_{\mathrm{opt}}$, is provided in the following theorem.

Theorem 3.1. *For $K, N_T \to \infty$, the optimal coefficient vector minimizing the asymptotic average MSE of the users in the n^{th} cell for the POLY precoder in (3.21) is given by*

$$\boldsymbol{\mu}_{\mathrm{opt}} = \gamma_3\boldsymbol{\Pi}^{-1}\boldsymbol{\psi}, \tag{3.24}$$

where $\boldsymbol{\psi} = [\zeta, \zeta^2, \ldots, \zeta^{\mathcal{I}+1}]^T$, $[\boldsymbol{\Pi}]_{i,j} = \mathrm{Tr}\left\{\mathbf{D}_{nn}\right\}\zeta^{i+j} + \left(\mathrm{Tr}\left\{\mathbf{D}_{nn}\boldsymbol{\Delta}_n\right\} + \frac{\mathrm{Tr}\{\boldsymbol{\Sigma}_n\}+P_{\mathrm{AN}}}{N_T p}\right)\zeta^{i+j-1}$, $\boldsymbol{\Sigma}_n = \mathbb{E}[\tilde{\mathbf{n}}_n\tilde{\mathbf{n}}_n^H]$, $\boldsymbol{\Delta}_n = \mathrm{diag}\left\{\frac{\theta_{nn}^1}{\theta_{nn}^1+p_\tau\tau\beta_{nn}^1}, \cdots, \frac{\theta_{nn}^K}{\theta_{nn}^K+p_\tau\tau\beta_{nn}^K}\right\}$, and $P_{\mathrm{AN}} = q\mathbb{E}\left[\mathrm{Tr}\left\{\mathbf{G}_{nn}\mathbf{A}_n\mathbf{A}_n^H\mathbf{G}_{nn}^H\right\}\right]$. Furthermore, ζ^l denotes the l^{th}-order moment of the sum of the eigenvalues of $\hat{\bar{\mathbf{H}}}_{nn}\hat{\bar{\mathbf{H}}}_{nn}^H$, i.e., $\zeta^l = \lim_{K\to\infty}\frac{1}{K}\sum_{k=1}^K\lambda_k^l$, which converges to $\zeta^l = \sum_{i=0}^{l-1}\binom{l}{i}\binom{l}{i+1}\frac{\beta^i}{l}$ for $K \to \infty$ [73, Theorem 2]. Finally, γ_3 is chosen such that $\mathrm{Tr}\{\mathbf{F}_n^H\mathbf{F}_n\} = 1$ holds.

Proof. Please refer to Appendix B.5. □

We note that $\boldsymbol{\mu}_{\mathrm{opt}}$ does not depend on instantaneous channel estimates, and hence, can be computed offline.

3.3.3 Computational Complexity of Data Precoding

We compare the computational complexity of the considered data precoders in terms of the number of floating point operations (FLOPs) [74]. Each FLOP represents one scalar complex addition or multiplication. We assume that the coherence time of the channel is T symbol intervals of which τ are used for training and $T-\tau$ are used for data transmission. Hence, the complexity required for precoding in one coherence interval, consist of the complexity required for generating one precoding matrix and $T-\tau$ precoded vectors. A similar complexity analysis was conducted in [73, Section IV] for various selfish data precoders without AN injection at the BS. Since the AN injection does not affect the structure of the data precoders, we can directly adapt the results from [73, Section IV] to the case at hand. In particular, the selfish MF, the SZF/SRCI, and the CZF/CRCI precoders require $(2K-1)N_T(T-\tau)$, $0.5(K^2+K)(2N_T-1)+K^3+K^2+K+N_TK(2K-1)+(2K-1)N_T(T-\tau)$, and $0.5(\xi^2K^2+\xi K)(2N_T-1)+\xi^3K^3+\xi^2K^2+\xi K+N_T\xi K(2\xi K-1)+(2K-1)N_T(T-\tau)$ FLOPs per coherence interval, see [73, Section IV]. In contrast, for the POLY data precoder, we obtain for the overall computational complexity $(T-\tau)\left((\mathcal{I}+1)(2K-1)N_T+\mathcal{I}(2N_T-1)K\right)$ FLOPs, which assumes implementation of the precoding operation by Horner's rule [73, Section IV].

The above complexity expressions reveal that the additional complexity introduced by collaborative data precoders compared to selfish data precoders is at most a factor of ξ^3. In addition, the complexity savings achieved with the POLY data precoder compared to the SZF/SRCI data precoders increase with increasing K for a given T. We note however that, regardless of their complexity, POLY data precoders are attractive as they avoid the stability issues that may arise in fixed point implementations of large matrix inverses.

3.4 Linear AN Precoders for Secure Massive MIMO

In this section, we investigate the performance of selfish and collaborative NS (S/CNS) and random AN precoders. In addition, a novel POLY AN precoder is derived. To the best of the authors' knowledge, POLY AN precoding has not been considered in the literature before.

3.4.1 Analysis of Existing AN Precoders

For a given dimensionality of the AN precoder, L, the secrecy rate depends on the AN precoder only via the AN leakage, Q, given in (3.9), which affects the SINR of the MT. Furthermore, the optimal POLY data precoder coefficients in (3.24) are affected by the AN precoder via the leakage term P_{AN}. In this subsection, for $N_T \to \infty$, we will provide closed-form expressions for Q and P_{AN} for the SNS, CNS, and random AN precoders.

SNS AN Precoder

The SNS AN precoder of the n^{th} BS is given by [24]

$$\mathbf{A}_n = \mathbf{I}_{N_T} - \hat{\mathbf{H}}_{nn}^H \left(\hat{\mathbf{H}}_{nn}\hat{\mathbf{H}}_{nn}^H\right)^{-1} \hat{\mathbf{H}}_{nn}, \tag{3.25}$$

which has rank $L = N_T - K$ and exists only if $\beta < 1$. We divide the corresponding AN leakage Q_{SNS} into an inter-cell AN leakage Q_o^{SNS} and an intra-cell AN leakage Q_i^{SNS}, where $Q_{\mathrm{SNS}} = Q_o^{\mathrm{SNS}} + Q_i^{\mathrm{SNS}}$. For the SNS AN precoder, Q_o^{SNS} is obtained as

$$\begin{aligned} Q_o^{\mathrm{SNS}} &= \sum_{m \in \mathcal{M}_n} \beta_{mn}^k \mathbb{E}\left[\mathbf{h}_{mn}^k \mathbf{A}_m \mathbf{A}_m^H (\mathbf{h}_{mn}^k)^H\right] + \sum_{m \notin \mathcal{M}_n \bigcup \{n\}} \beta_{mn}^k \mathbb{E}\left[\mathbf{h}_{mn}^k \mathbf{A}_m \mathbf{A}_m^H (\mathbf{h}_{mn}^k)^H\right] \\ &= \mathbb{E}\left[\mathrm{tr}\left\{\mathbf{A}_m \mathbf{A}_m^H\right\}\right] \left(\sum_{m \in \mathcal{M}_n} \mu_{mk} + \sum_{m \notin \mathcal{M}_n \bigcup \{n\}} \beta_{mn}^k \right) \\ &= (N_T - K) \left(\sum_{m \in \mathcal{M}_n} \mu_{mk} + \sum_{m \notin \mathcal{M}_n \bigcup \{n\}} \beta_{mn}^k \right), \end{aligned} \tag{3.26}$$

where we exploited [71, Lemma 11] and the independence of $\mathbf{A}_m$ and $\tilde{\mathbf{h}}_{mn}^k$ (for contaminated cells, i.e., $m \in \mathcal{M}_n$) and $\mathbf{h}_{mn}^k$ (for non-contaminated cells, i.e., $m \notin \mathcal{M}_n \bigcup \{n\}$). In contrast, the intra-cell AN leakage power is given by

$$Q_i^{\mathrm{SNS}} = \beta_{nn}^k \mathbb{E}\left[\mathbf{h}_{nn}^k \mathbf{A}_n \mathbf{A}_n^H (\mathbf{h}_{nn}^k)^H\right] = \beta_{nn}^k \mathbb{E}\left[\tilde{\mathbf{h}}_{nn}^k \mathbf{A}_n \mathbf{A}_n^H (\tilde{\mathbf{h}}_{nn}^k)^H\right] = (N_T - K)\mu_{nk}, \tag{3.27}$$

as the SNS AN precoder matrix lies in the NS of the estimated channels of all K MTs in the n^{th} cell. Similarly, the AN leakage relevant for computation of the POLY data precoder is obtained as

$$P_{\mathrm{AN}}^{\mathrm{SNS}} = (1 - \phi) P_T \lim_{K \to \infty} \frac{1}{K} \sum_{k=1}^{K} \mu_{nk}. \tag{3.28}$$

CNS AN Precoder

For the CNS AN precoder at the n^{th} BS, the AN is designed to lie in the NS of the estimated channels between all MK MTs and the BS, i.e.,

$$\mathbf{A}_n = \mathbf{I}_{N_T} - \hat{\mathbf{H}}_n^H \left(\hat{\mathbf{H}}_n \hat{\mathbf{H}}_n^H \right)^{-1} \hat{\mathbf{H}}_n, \tag{3.29}$$

which has rank $L = N_T - \xi K$ and exists only if $\beta < 1/\xi$. The corresponding AN leakage to the k^{th} MT in the n^{th} cell is given by

$$Q_{\text{CNS}} = \sum_{m=1}^{M} \beta_{mn}^{k} \mathbb{E}\Big[\mathbf{h}_{mn}^{k} \mathbf{A}_m \mathbf{A}_m^H (\mathbf{h}_{mn}^{k})^H \Big] = (N_T - \xi K) \sum_{m=1}^{M} \mu_{mk}. \tag{3.30}$$

Furthermore, the CNS AN precoder results in the same P_{AN} as the SNS AN precoder, cf. (3.28).

Random AN Precoder

For the random precoder, all elements of $\mathbf{A}_n$ are i.i.d. r.v.s independent of the channel [43], i.e., $\mathbf{A}_n$ has rank $L = N_T$. Hence, $\mathbf{h}_{mn}^{k}$ and $\mathbf{A}_m$, $\forall m$, are mutually independent, and we obtain

$$Q_{\text{random}} = \sum_{m=1}^{M} \beta_{mn}^{k} \mathbb{E}\Big[\mathbf{h}_{mn}^{k} \mathbf{A}_m \mathbf{A}_m^H (\mathbf{h}_{mn}^{k})^H \Big] = N_T \sum_{m=1}^{M} \beta_{mn}^{k}. \tag{3.31}$$

Furthermore, we obtain $P_{\text{AN}}^{\text{random}} = (1-\phi) P_T \lim_{K\to\infty} \frac{1}{K} \sum_{k=1}^{K} \beta_{nn}^{k}$.

Remark 3.3. *If the power and time allocated to channel estimation are very small, i.e., $\tau p_\tau \to 0$, the S/CNS AN precoders yield the same qQ and P_{AN} as the random AN precoder. This suggests that in this regime all considered AN precoders achieve a similar SINR performance for a given MT. However, for $\tau p_\tau > 0$, the S/CNS AN* *precoders cause less AN leakage resulting in an improved SINR performance compared to the random precoder at the expense of a higher complexity.*

3.4.2 POLY AN Precoder

To mitigate the high computational complexity imposed by the matrix inversion required for the S/CNS AN precoders, while achieving an improved performance compared to the random AN precoder, we propose a POLY AN precoder. Similar to the POLY data precoder, we concentrate on the selfish design because of the desired low complexity, and hence, set $L = N_T - K$. The proposed POLY AN precoder is given by

$$\mathbf{A}_n = \mathbf{I}_{N_T} - \hat{\bar{\mathbf{H}}}_{nn}^H \left(\sum_{i=0}^{\mathcal{J}} \nu_j \left(\hat{\bar{\mathbf{H}}}_{nn} \hat{\bar{\mathbf{H}}}_{nn}^H \right)^j \right) \hat{\bar{\mathbf{H}}}_{nn}, \tag{3.32}$$

where $\boldsymbol{\nu} = [\nu_0, \ldots, \nu_{\mathcal{J}}]^T$ contains the real-valued coefficients of the AN precoder polynomial, which have to be optimized. In particular, $\boldsymbol{\nu}$ is optimized for minimization of the asymptotic average AN leakage caused to all MTs in the n^{th} cell P_{AN}. The corresponding optimization problem is formulated as

$$\min_{\boldsymbol{\nu}} P_{\text{AN}} = q\mathbb{E}\left[\text{Tr}\{\mathbf{G}_{nn}\mathbf{A}_n\mathbf{A}_n^H\mathbf{G}_{nn}^H\} \right] \quad \text{s.t. :} \text{Tr}\{\mathbf{A}_n^H\mathbf{A}_n\} = 1/\beta - 1. \tag{3.33}$$

The solution of (3.33) is provided in the following theorem.

Theorem 3.2. *For $K, N_T \to \infty$, the optimal coefficient vector minimizing the asymptotic average AN leakage caused to the users in the n^{th} cell for the AN precoder structure in (3.32) is given by*

$$\boldsymbol{\nu}_{\text{opt}} = \boldsymbol{\Sigma}^{-1}\boldsymbol{\omega}, \tag{3.34}$$

where $[\boldsymbol{\Sigma}]_{i,j} = \zeta^{i+j+1} + \epsilon\zeta^{i+j}$ and $\boldsymbol{\omega} = [\zeta^2 + \epsilon\zeta, \ldots, \zeta^{\mathcal{J}+2} + \epsilon\zeta^{\mathcal{J}+1}]$. Here, ζ^l de-

notes again the l^{th} order moment of the sum of the eigenvalues of matrix $\hat{\bar{\mathbf{H}}}_{nn}\hat{\bar{\mathbf{H}}}_{nn}^H$, cf. Theorem 3.1. ϵ is chosen such that $\mathrm{Tr}\{\mathbf{A}_n^H\mathbf{A}_n\} = 1/\beta - 1$.

Proof. Please refer to Appendix B.6. □

3.4.3 Computational Complexity of AN Precoding

Similarly to the data precoders, the complexity of the AN precoders is evaluated in terms of the number of flops required per coherence interval T. For the SNS AN precoder, the computation of $\mathbf{A}_n$ in (3.25) requires the computation and inversion of a $K \times K$ positive definite matrix, which entails $0.5(K^2+K)(2N_T-1)+K^3+K^2+K$ FLOPs [74], and the multiplication of an $N_T \times K$, an $K \times K$, and an $K \times N_T$ matrix, which entails $N_T(N_T+K)(2K-1)$ FLOPs [74]. Furthermore, the $T-\tau$ vector-matrix multiplications required for AN precoding entail a complexity of $(2N_T-1)N_T$ FLOPs [74], respectively. Hence, the overall complexity is $0.5(K^2+K)(2N_T-1)+K^3+K^2+K+N_T(N_T+K)(2K-1)+(2N_T-1)N_T(T-\tau)$ FLOPs. Similarly, for the CNS AN precoder, we obtain a complexity of $0.5(\xi^2K^2+\xi K(2N_T-1)+\xi^3K^3+\xi^2K^2+\xi K+N_T(N_T+\xi K)(2\xi K-1)+(2N_T-1)N_T(T-\tau)$ FLOPs, whereas the random AN precoder entails a complexity of $(2N_T-1)N_T(T-\tau)$ FLOPs as only the AN vector-matrix multiplications are required.

Similar to the precoded data vector [73, Section IV], the POLY precoded AN vector can be generated using Horner's rule. Hence, based on (3.32), the transmitted AN vector in the n^{th} cell can be obtained as

$$\mathbf{A}_n\mathbf{z}_n = \mathbf{z}_n - \left(\nu_0\hat{\bar{\mathbf{H}}}_{nn}^H\hat{\bar{\mathbf{H}}}_{nn}\left(\mathbf{z}_n + \frac{\nu_1}{\nu_0}\hat{\bar{\mathbf{H}}}_{nn}^H\hat{\bar{\mathbf{H}}}_{nn}\left(\mathbf{z}_n + \ldots\right)\right)\right). \qquad (3.35)$$

Hence, $\mathbf{A}_n\mathbf{z}_n$ can be computed efficiently by first multiplying $\mathbf{H}_{nn}$ with $\mathbf{z}_n$, which requires $(2N_T-1)K$ FLOPs, then multiplying $\hat{\mathbf{H}}_{nn}^H$ with the resulting vector, which requires $(2K-1)N_T$ FLOPs, adding $\mathbf{z}_n$ to the resulting vector, and repeating similar operations $(\mathcal{J}+1)$ times, see [16, 73] for details on Horner's rule. Overall, this leads to a complexity of $(\mathcal{J}+1)\left((2K-1)N_T+(2N_T-1)K\right)(T-\tau)$ FLOPs.

3.5 Comparison of Linear Data and AN Precoders

In this subsection, we compare the secrecy performances of the considered data and AN precoders. Thereby, in order to get tractable results, we focus on the relative performances of SZF, CZF, and MF, cf. Chapter 2 data precoders and SNS, CNS, and random AN precoders. The performances of SRCI, CRCI, and POLY data precoders and the POLY AN precoder will be investigated via numerical and simulation results in Section 3.6.

In order to gain some insight for system design and analysis, we adopt a simplified path-loss model. In particular, we assume the path losses are given by

$$\beta_{mn}^k = \begin{cases} 1, & m=n \\ \rho, & \text{otherwise} \end{cases} \tag{3.36}$$

where $\rho \in [0,1]$ denotes the inter-cell interference factor. For this simplified model, a and c in (3.8) simplify to $a = 1+(M-1)\rho$ and $c = 1+(M-1)\rho^2$. Furthermore, the SINR expressions of the linear data precoders considered in Section 3.3.1 and the MF precoder considered in Chapter 2 can be simplified considerably and are provided in Table 3.1, where we use the normalized AN leakage $\tilde{Q} = Q/L$. The expressions for the normalized AN leakage $\tilde{Q}$, the asymptotic average AN leakage P_{AN}, and the dimensionality L of the considered linear AN precoders are given in Table 3.2. Under the simplified model, λ_{mk} defined in Proposition 3.1 simplifies to

$$\begin{cases} \lambda_1 = \frac{p_\tau \tau}{1+(1+|\mathcal{M}_n|\rho)p_\tau \tau} = \frac{p_\tau \tau}{1+bp_\tau \tau}, & \text{for } m = n \\ \rho^2\lambda_1 = \frac{\rho^2 p_\tau \tau}{1+bp_\tau \tau}, & \text{for } m \in \mathcal{M}_n \\ \rho^2\lambda_2 = \frac{\rho^2 p_\tau \tau}{1+(|\mathcal{M}_n|+1)\rho p_\tau \tau}, & \text{for } m \notin \mathcal{M}_n \bigcup\{n\} \end{cases} \tag{3.37}$$

with $b = 1 + |\mathcal{M}_n|\rho$. Accordingly, the term $\sum_{m\in\mathcal{M}_n\cup\{n\}} \mu_{mk}$ and $\sum_{m=1}^{M} \mu_{mk}$ in Propositions 3.1 and 3.2 simplify to $b - d\lambda_1$ and $a - d\lambda_1 - (c-d)\lambda_2$, respectively, where $d = 1 + |\mathcal{M}_n|\rho^2$. By combining all above intermediate results, $\hat{\Gamma}^m_{\text{SRCI}}$ and $\hat{\Gamma}^m_{\text{CRCI}}, 1 \le m \le M$, simplify to

$$\hat{\Gamma}^m_{\text{SRCI}} = \begin{cases} \hat{\Gamma}_{\text{SRCI}}, & \text{for } m = n \\ \rho^2\hat{\Gamma}_{\text{SRCI}}, & \text{for } m \in \mathcal{M}_n \end{cases}, \ \hat{\Gamma}^m_{\text{CRCI}} = \begin{cases} \hat{\Gamma}_{\text{CRCI}}, & \text{for } m = n \\ \rho^2\hat{\Gamma}_{\text{SRCI}}, & \text{for } m \in \mathcal{M}_n \\ \rho^2\lambda_2/\lambda_1\hat{\Gamma}_{\text{SRCI}}, & \text{for } m \notin \mathcal{M}_n \cup \{n\} \end{cases}, \tag{3.38}$$

respectively, where

$$\hat{\Gamma}_{\text{SRCI}} = \frac{\Gamma_{\text{SRCI}}\lambda_1}{\Gamma_{\text{SRCI}}(b - d\lambda_1) + 1}, \quad \hat{\Gamma}_{\text{CRCI}} = \frac{\Gamma_{\text{CRCI}}\lambda_1}{\Gamma_{\text{CRCI}}\left(a - d\lambda_1 - (c-d)\lambda_2\right) + 1}, \tag{3.39}$$

and

$$\Gamma_{\text{SRCI}} = \frac{\beta\phi}{\beta\phi(a-b) + (1-\phi)\beta\tilde{Q} + \frac{\beta}{P_T}}, \quad \Gamma_{\text{CRCI}} = \frac{\beta\phi}{(1-\phi)\beta\tilde{Q} + \frac{\beta}{P_T}}. \tag{3.40}$$

Table 3.1: SINR of the k^{th} MT in the n^{th} cell for linear data precoding and the simplified path-loss model in (3.36).

Data Precoder	γ_{nk}
SZF	$\frac{\lambda_1\phi(1-\beta)}{(1-\phi)\beta\tilde{Q}+\beta\phi(a-d\lambda_1)+(d-1)\lambda_1\phi(1-\beta)+\beta/P_T}$
SRCI	$\frac{1}{1/d\mathcal{G}(\beta,\beta/d\hat{\Gamma}_{\text{SRCI}})+d-1}$
CZF	$\frac{\lambda_1\phi(1-\xi\beta)}{(1-\phi)\beta\tilde{Q}+\beta\phi(a-d\lambda_1-(c-d)\lambda_2)+(d-1)\lambda_1\phi(1-\xi\beta)+\beta/P_T}$
CRCI	$\frac{1}{1/(d+(c-d)\lambda_2/\lambda_1)\mathcal{G}(\xi\beta,\xi\beta/(d+(c-d)\lambda_2/\lambda_1)\hat{\Gamma}_{\text{CRCI}})+d-1}$
MF	$\frac{\lambda_1\phi}{(1-\phi)\beta\tilde{Q}+\beta\phi a+(d-1)\lambda_1\phi+\beta/P_T}$

Table 3.2: AN leakage for simplified path-loss model in (3.36).

AN Precoder	$\tilde{Q}$	P_{AN}	L
SNS	$a - d\lambda_1$	$(1-\phi)P_T(1-\lambda_1)$	$N_T - K$
CNS	$a - d\lambda_1 - (c-d)\lambda_2$	$(1-\phi)P_T(1-\lambda 1)$	$N_T - \xi K$
Random	a	$(1-\phi)P_T$	N_T

3.5.1 Comparison of SZF, CZF, and MF Data Precoders

In this subsection, we compare the performances achieved with SZF, CZF, and MF data precoders for a given AN precoder, i.e., L and $\tilde{Q}$ are fixed. Since the upper bound on the capacity of the eavesdropper channel is independent of the adopted data precoder, cf. Section 3.2.3, we compare the considered data precoders based on their SINRs. Exploiting the results in Table 3.1, we obtain the following relations between γ_{nk}^{SZF}, γ_{nk}^{CZF}, and γ_{nk}^{MF}:

$$\begin{aligned}
\frac{\gamma_{nk}^{\text{SZF}}}{\gamma_{nk}^{\text{MF}}} &= 1 + \beta((d + |\mathcal{M}_n|\rho^2)\gamma_{nk}^{\text{SZF}} - 1) \\
\frac{\gamma_{nk}^{\text{CZF}}}{\gamma_{nk}^{\text{SZF}}} &= \frac{1-\xi\beta}{1-\beta} + \frac{[(c-d)\lambda_2/\lambda_1 + (d-1)(\xi-1)]\beta}{1-\beta}\gamma_{nk}^{\text{CZF}}.
\end{aligned} \tag{3.41}$$

Hence, for $\gamma_{nk}^{\text{SZF}} > \gamma_{nk}^{\text{MF}}$, we require $\gamma_{nk}^{\text{SZF}} > 1/(d + |\mathcal{M}_n|\rho^2) = 1/(1 + 2\rho^2|\mathcal{M}_n|)$, and for $\gamma_{nk}^{\text{CZF}} > \gamma_{nk}^{\text{SZF}}$, we need $\gamma_{nk}^{\text{CZF}} > (\xi-1)/((c-d)\lambda_2/\lambda_1 + (d-1)(\xi-1))$. As expected, (3.41) suggests that for a lightly loaded system, i.e., $\beta \to 0$, all three precoders have a similar performance, i.e., $\gamma_{nk}^{\mathrm{CZF}} \approx \gamma_{nk}^{\mathrm{SZF}} \approx \gamma_{nk}^{\mathrm{MF}}$. Moreover, when $\xi = 1$, we simply have $\gamma_{nk}^{\mathrm{CZF}} = \gamma_{nk}^{\mathrm{SZF}}$, as SZF and CZF are equivalent, cf. Remark 3.1. In the following, we investigate the impact of the number of MTs and the pilot power on the relative performances of the considered data precoders.

Number of MTs: From (3.41), we find that for $\gamma_{nk}^{\mathrm{SZF}} > \gamma_{nk}^{\mathrm{MF}}$ and $\gamma_{nk}^{\mathrm{CZF}} > \gamma_{nk}^{\mathrm{SZF}}$ to hold, the number of MTs has to meet $K < K_{\mathrm{SZF>MF}}$ and $K < K_{\mathrm{CZF>SZF}}$, where

$$\begin{aligned} K_{\mathrm{SZF>MF}} &= \frac{d\lambda_1 \phi N_T}{(1-\phi)\tilde{Q} + a\phi + 1/P_T} \\ K_{\mathrm{CZF>SZF}} &= \frac{\phi(c-d)\lambda_2 N_T}{(1-\phi)(\xi-1)\tilde{Q} + ((a-d\lambda_1)(\xi-1) + (c-d)\lambda_2)\phi + (\xi-1)/P_T}, \end{aligned} \tag{3.42}$$

for $\xi > 1$, respectively. Interestingly, both the maximum numbers of MTs for which the SZF data precoder is advantageous compared to the MF data precoder, $K_{\mathrm{SZF>MF}}$, and the maximum number of MTs for which the CZF data precoder is advantageous compared to the SZF data precoder, $K_{\mathrm{CZF>SZF}}$, decrease with increasing AN leakage, $\tilde{Q}$, the number of cells M and the number of contaminated neighboring cells $|\mathcal{M}_n|$ (via d), but increase with the amount of resources dedicated to channel estimation, $p_\tau \tau$ (via λ_1 and λ_2), and consequently with the channel estimation quality. However, while $K_{\mathrm{SZF>MF}}$ decreases with increasing inter-cell interference factor ρ (via a, c, and d), $K_{\mathrm{CZF>SZF}}$ increases.

3.5.2 Comparison of SNS, CNS, and Random AN Precoders

In this subsection, we analyze the impact of the AN precoders on the secrecy rate. AN precoders affect the ergodic capacity of the eavesdropper via L and the achievable rate of the MT via the leakage, $\tilde{Q}$. Since the upper bound on the ergodic secrecy rate of the eavesdropper in (3.8) is a decreasing function in L, we have

$$C_{nk}^{\text{eve}}|_{\text{random}} \leq C_{nk}^{\text{eve}}|_{\text{SNS}} \leq C_{nk}^{\text{eve}}|_{\text{CNS}}. \tag{3.43}$$

On the other hand, from Table 3.2, we observe $\tilde{Q}_{\text{random}} \geq \tilde{Q}_{\text{SNS}} \geq \tilde{Q}_{\text{CNS}}$. Since according to Table 3.1 the SINRs for all data precoders are decreasing functions of $\tilde{Q}$, for a given data precoder, we obtain for the lower bound on the ergodic rate of the k^{th} MT in the n^{th} cell

$$R_{nk}|_{\text{random}} \leq R_{nk}|_{\text{SNS}} \leq R_{nk}|_{\text{CNS}}. \tag{3.44}$$

Considering (3.43), (3.44), and the expression for the ergodic secrecy rate, $R_{nk}^{\text{sec}} = [R_{nk} - C_{nk}^{\text{eve}}]^{+}$, it is not a priori clear which AN precoder has the best performance. In fact, our numerical results in Section 3.6 confirm that it depends on the system parameters (e.g. α, β, M, ξ, $p_\tau \tau$, and ρ) which AN precoder is preferable.

3.5.3 Ergodic Secrecy Rate Analysis

In this subsection, we provide closed-form results for the ergodic secrecy rate for SZF, CZF, and MF data precoding for the simplified path-loss model in (3.36). Thereby, the simplified path-loss model is extended also to the eavesdropper, i.e., $\beta_{nE} = 1$ and $\beta_{mE} = \rho$, $m \neq n$, is assumed.

Combining (3.5), (3.8), and the results in Table 3.1, we obtain the following lower bounds for the ergodic secrecy rate of the k^{th} MT in the n^{th} cell:

$$R_{nk}^{\text{sec}} \geq \begin{cases} \left[\log_2\left(\frac{(\tilde{Q}+1/P_T)\beta+(a-\tilde{Q})\beta\phi+d\lambda_1\phi}{(\tilde{Q}+1/P_T)\beta+(a-\tilde{Q})\beta\phi+(d-1)\lambda_1\phi}\cdot\frac{-\chi\phi+\chi}{(1-\chi)\phi+\chi}\right)\right]^+ & \text{MF}, \\ \left[\log_2\left(\frac{(\tilde{Q}+1/P_T)\beta+(a-d\lambda_1-\tilde{Q})\beta\phi+d\lambda_1(1-\beta)\phi}{(\tilde{Q}+1/P_T)\beta+(a-d\lambda_1-\tilde{Q})\beta\phi+(d-1)\lambda_1(1-\beta)\phi}\cdot\frac{-\chi\phi+\chi}{(1-\chi)\phi+\chi}\right)\right]^+ & \text{SZF}, \\ \left[\log_2\left(\frac{(\tilde{Q}+1/P_T)\beta+(a-d\lambda_1-(c-d)\lambda_2-\tilde{Q})\beta\phi+d\lambda_1(1-\xi\beta)\phi}{(\tilde{Q}+1/P_T)\beta+(a-d\lambda_1-(c-d)\lambda_2-\tilde{Q})\beta\phi+(d-1)\lambda_1(1-\xi\beta)\phi}\cdot\frac{-\chi\phi+\chi}{(1-\chi)\phi+\chi}\right)\right]^+ & \text{CZF}, \end{cases} \tag{3.45}$$

where $\chi = \frac{a\beta}{\alpha} - \frac{\beta c N_T}{aL}$, and $\tilde{Q}$ and L are given in Table 3.2 for the considered AN precoders. Eq. (3.45) is easy to evaluate and reveals how the ergodic secrecy rate of the three considered data precoders depends on the various system parameters. To gain more insight, we determine the maximum value of α which admits a non-zero secrecy rate. This value is denoted by α_s in the following, and can be shown to be a decreasing function of ϕ for all conidered data precoders. Hence, we find α_s by setting $R_{nk}^{\text{sec}} = 0$ in (3.45) and letting $\phi \to 0$. This leads to

$$\alpha_s = \begin{cases} \frac{a^2\lambda_1}{\tilde{Q}a+d\lambda_1 N_T/L+a/P_T} & \text{for MF} \\ \frac{(1-\beta)a^2\lambda_1}{\tilde{Q}a+d\lambda_1(1-\beta)N_T/L+a/P_T} & \text{for SZF}, \\ \frac{(1-\xi\beta)a^2\lambda_1}{\tilde{Q}a+d\lambda_1(1-\xi\beta)N_T/L+a/P_T} & \text{for CZF}. \end{cases} \tag{3.46}$$

Eq. (3.46) reveals that for a given AN precoder, independent of the system parameters, the MF data precoder can always tolerate a larger number of eavesdropper antennas than the SZF data precoder, which in turn can always tolerate a larger number of eavesdropper antennas than the CZF data precoder. This can be explained by the fact that the high AN transmit power required to combat a large number of eavesdropper antennas drives the receiver of the desired MT into the noise-limited regime, where the MF data precoder has a superior performance compared to the

S/CZF data precoders. On the other hand, since α_s depends on both $\tilde{Q}$ and L, it is not a priori clear which AN precoder can tolerate the largest number of eavesdropper antennas. For a lightly loaded network with small β and small M, according to Table 3.2, we have $L \approx N_T$ for all three AN precoders. Hence, in this case, we expect the CNS AN precoder to outperform the SNS and random AN precoders as it achieves a smaller $\tilde{Q}$. On the other hand, for a heavily loaded network with large β and M, the value of α_s of the CNS AN precoder is compromised by its small value of L and SNS and even random AN precoders are expected to achieve a larger α_s.

3.6 Performance Evaluation

In this section, we evaluate the performance of the considered secure multi-cell massive MIMO system. We consider cellular systems with $M = 2$ and $M = 7$ hexagonal cells, respectively, and to gain insight for system design, we adopt the simplified path-loss model introduced in Section 3.5, i.e., the severeness of the inter-cell interference is only characterized by the parameter $\rho \in (0, 1]$. Various pilot contamination patterns are considered by having different pilot length $\tau = \xi K, \xi \in \mathcal{M}$. The simulation results for the ergodic secrecy rate of the k^{th} MT in the n^{th} cell are based on (3.5), (3.7), and the expression for the ergodic rate of the MT [43, Eq. (8)] and are averaged over $5,000$ random channel realizations. Note that, in this chapter, we consider the ergodic secrecy rate of a certain MT, i.e., the k^{th} MT in the n^{th} cell. The cell sum secrecy rate can be obtained by multiplying the secrecy rate of the k^{th} MT by the number of MTs, K, as for the considered channel model, all MTs in the n^{th} cell achieve the same secrecy rate. The values of all relevant system parameters are provided in the captions of the figures. To enable a fair comparison, throughout this section, we adopted the SNS AN precoder when we compare different data precoders and the SZF data precoder when we compare different AN precoders.

3.6.1 Ergodic Capacity of the Eavesdropper for Conventional Linear AN Precoders

In Fig. 3.1, we show the ergodic capacity of the eavesdropper for the considered conventional AN precoders. First, we note that the upper bound in (3.8) is very tight for all AN precoders and all consider values of α and β. Furthermore, as β increases, the ergodic capacity of all AN precoders decreases since the power allocated to the information-carrying signal of the user that the eavesdropper tries to intercept decreases with increasing β as the total power allocated to the information-carrying signals of all users is fixed. As expected, the eavesdropper's capacity benefits from larger values of α. Furthermore, as predicted in (3.43), because of their different values of L, the CNS AN precoder yields the largest eavesdropper capacity, while the random AN precoder yields the lowest. The performance differences between the different AN precoders diminish for small values of α and β as the dependence of the eavesdropper capacity on L becomes negligible for small α, cf. (3.8), and $L \approx N_T$ holds for all precoders for small β, cf. Table 3.2.

3.6.2 Ergodic Secrecy Rate for Conventional Linear Data Precoders

In Figs. 3.2 and 3.3, we show the ergodic secrecy rates of the k^{th} MT in the n^{th} cell vs. the number of BS antennas for the MF, SZF, CZF, SRCI, and CRCI data precoders for a lightly loaded and a dense network, respectively, and a fixed power allocation factor of $\phi = 0.75$. In both figures, the analytical results were obtained from (3.5), (3.7), and (3.15) for the SRCI data precoder, (3.19) for the CRCI data

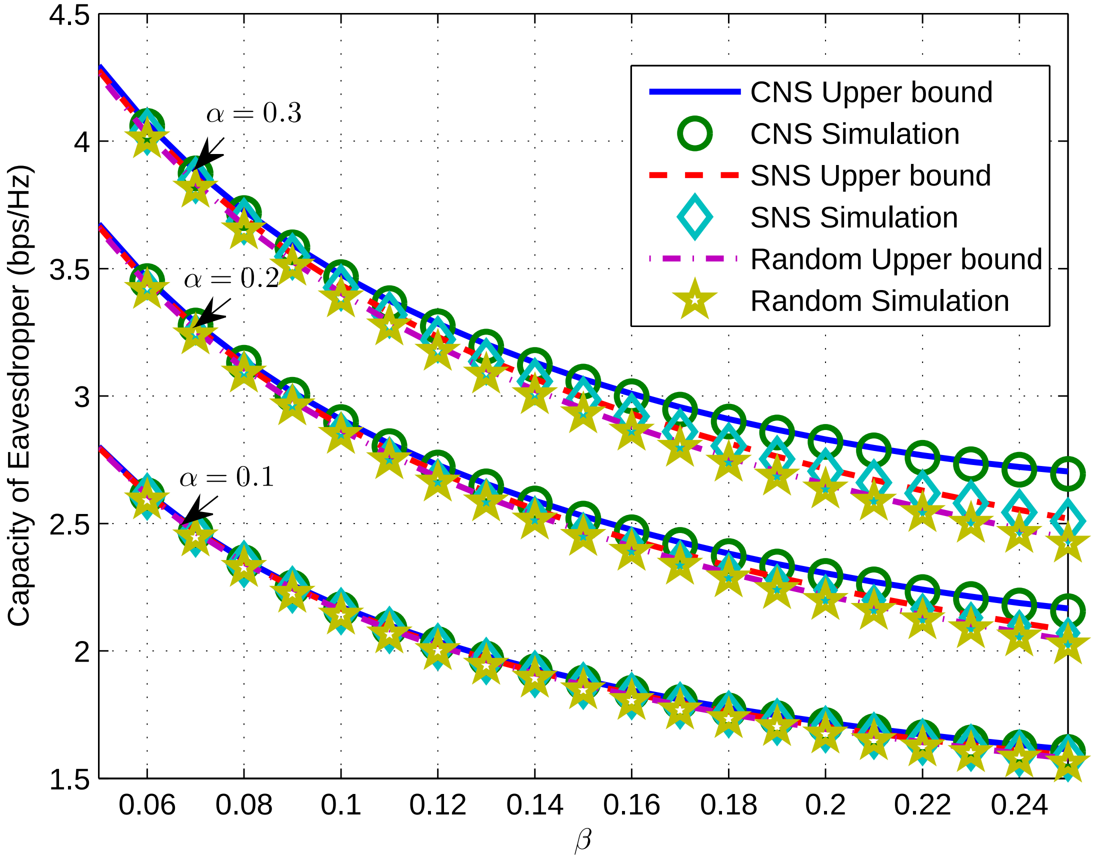

Figure 3.1: Ergodic capacity of the eavesdropper vs. the normalized number of MTs in the cell, β, for a system with $N_T = 200$, $\phi = 0.75$, $P_T = 10$ dB, $\rho = 0.3$, and $M = \xi = 2$.

precoder, and (3.45) for the MF, SZF, and CZF data precoders. For all considered precoders, the analytical results provide a tight lower bound for the ergodic secrecy rates obtained by simulations. Furthermore, as expected, the RCI data precoders outperform the ZF data precoders for both the selfish and the collaborative strategies, but the performance gap diminishes with increasing number of BS antennas.

For the lightly loaded network in Fig. 3.2, we assume $M = 2$ cells with no pilot contamination, i.e., $\xi = 2$, and $K = 10$ users with a small inter-cell interference factor of $\rho = 0.1$. For this scenario, the collaborative designs outperform the selfish designs

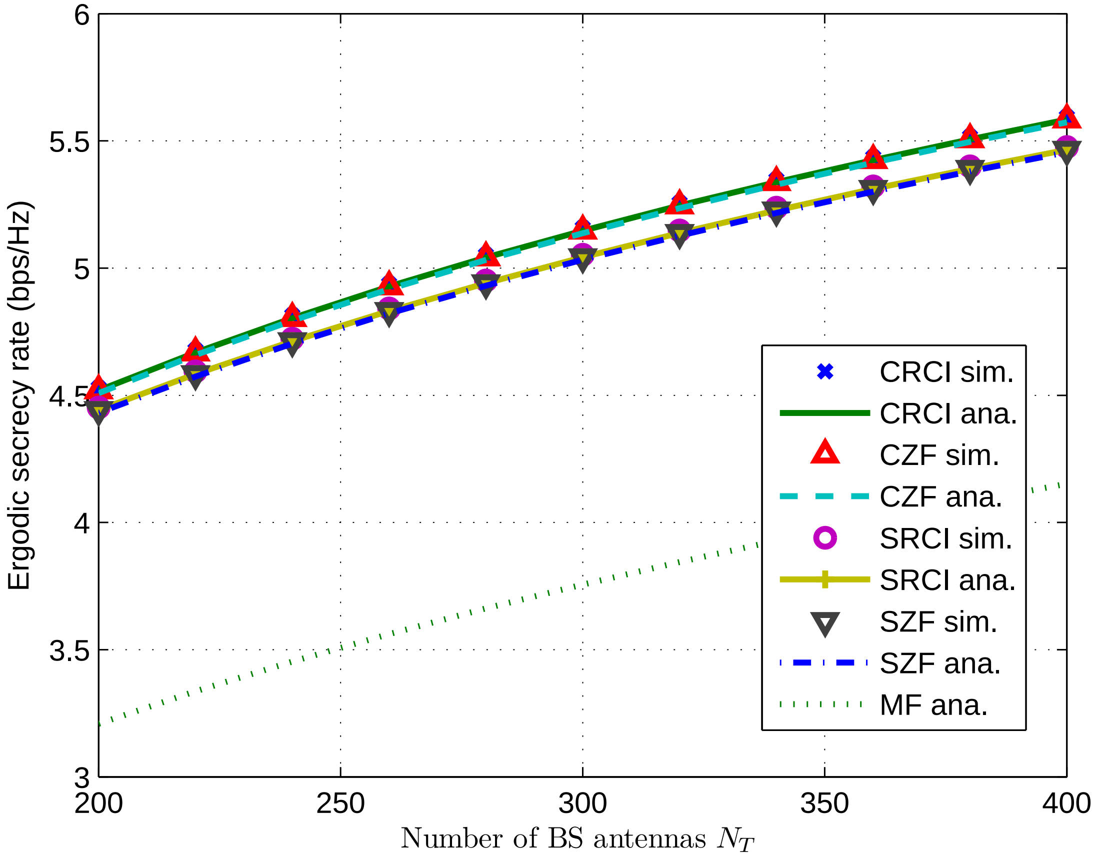

Figure 3.2: Analytical and simulation results for the ergodic secrecy rate vs. the number of BS antennas, N_T, for a lightly loaded network with $\phi = 0.75$, $P_T = 10$ dB, $p_\tau = P_T/\tau$, $\alpha = 0.1$, $K = 10$, $\rho = 0.1$, and $M = \xi = 2$.

and C/SZF precoding yield a large performance gain compared to MF precoding. This is expected from our analysis in Section 3.5.1 as for the parameters valid for Fig. 3.2, we obtain from (3.42), $K_{\text{SZF>MF}} \approx 280$ and $K_{\text{CZF>SZF}} \approx 46$ for $N_T = 400$. Intuitively, as the network is only lightly loaded and without pilot contamination, the collaborative data precoder can efficiently reduce interference to the other cell despite the expense of spatial degrees of freedom.

For the dense network in Fig. 3.3, we assume $M = 7$ cells, $\xi = 2$, $K = 40$ users, and a larger inter-cell interference factor of $\rho = 0.3$. In this case, for the considered range of N_T, the collaborative precoder designs are not able to suppress inter-cell

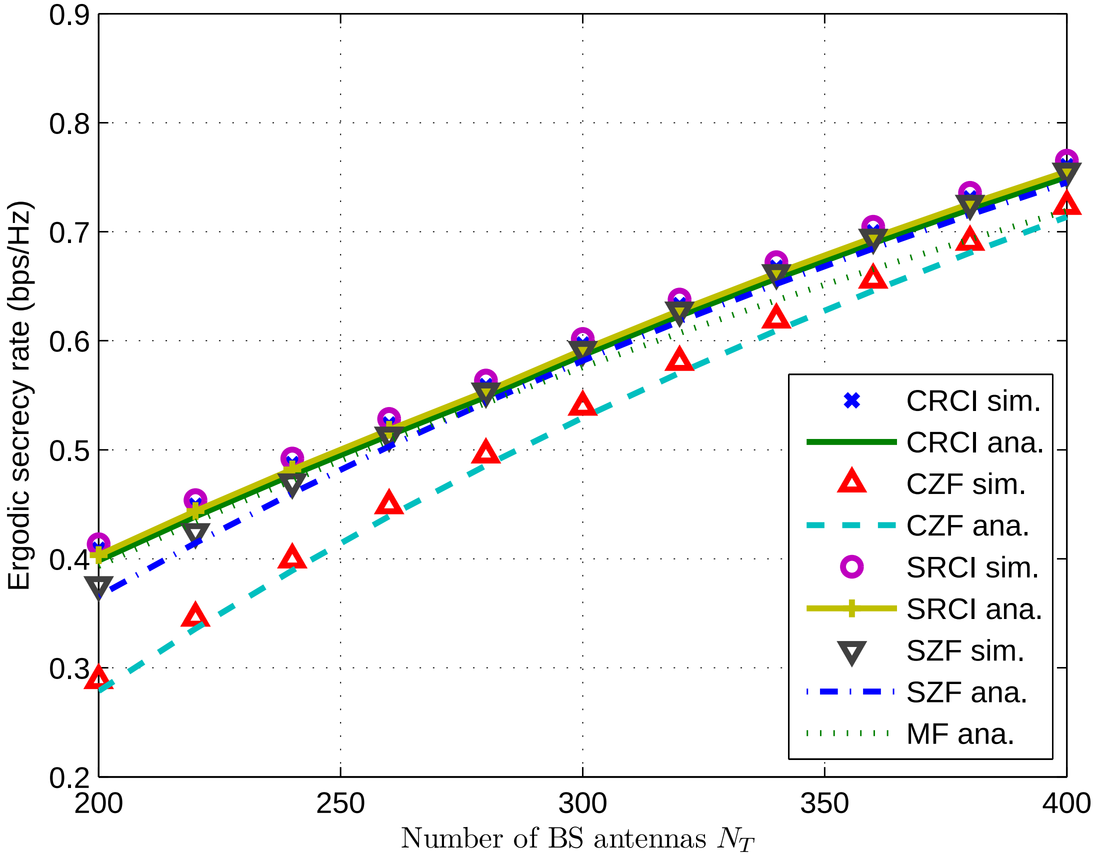

Figure 3.3: Analytical and simulation results for the ergodic secrecy rate vs. the number of BS antennas, N_T, for a dense network with $\phi = 0.75$, $P_T = 10$ dB, $\xi = 2$, $p_\tau = P_T/\tau$, $\alpha = 0.1$, $K = 40$, $\rho = 0.3$, and $M = 7$.

interference and AN leakage to other cells sufficiently well to outperform the selfish precoder designs. In fact, for $N_T = 400$, we obtain from (3.42) $K_{\text{CZF}>\text{SZF}} \approx 26$, i.e., our analytical results suggest that the SZF precoder outperforms the CZF precoder for $K = 40$ which is confirmed by Fig. 3.3. Nevertheless, for $N_T > 400$, the ergodic secrecy rate for the CZF data precoder will eventually surpass that for the SZF data precoder.

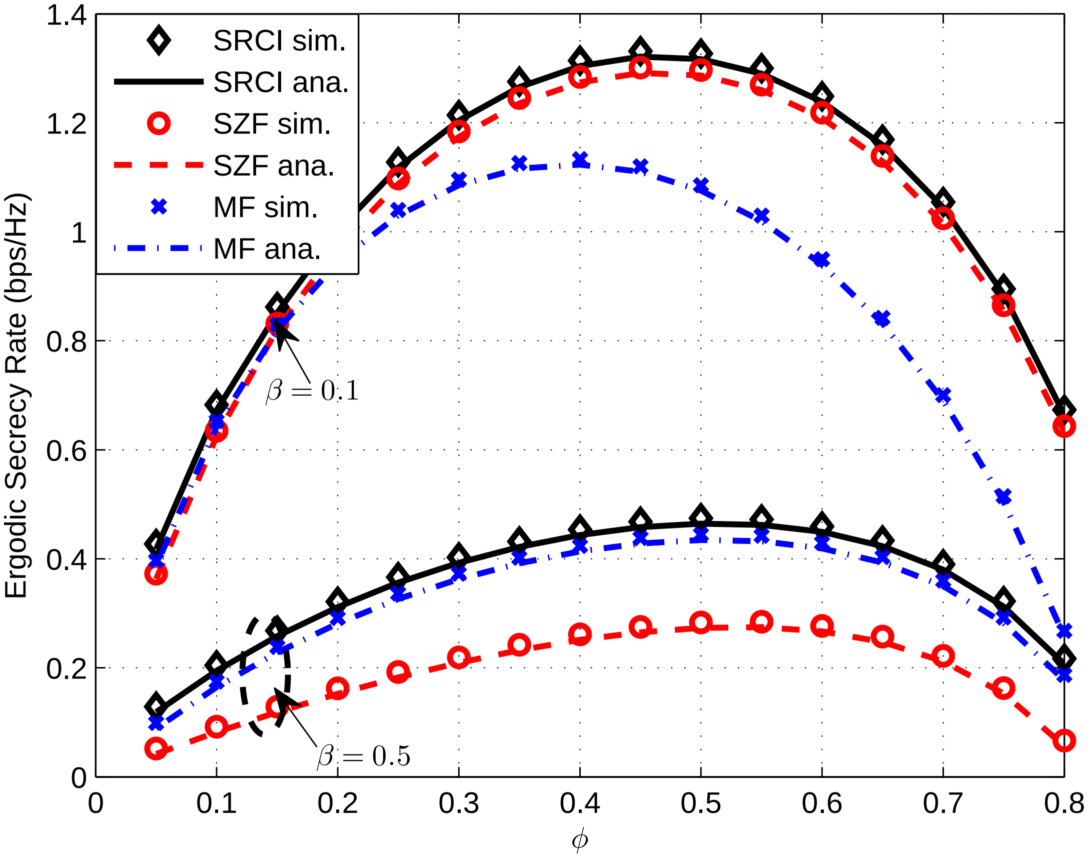

Figure 3.4: Ergodic secrecy rate vs. ϕ for different selfish data precoders for a network with $P_T = 10$ dB, $N_T = 100$, $\xi = 2$, $p_\tau = P_T/K$, $\alpha = 0.1$, $\rho = 0.1$, and $M = 7$.

3.6.3 Optimal Power Allocation

In this subsection, we investigate the dependence of the ergodic secrecy rate on the power allocation factor ϕ and study the impact of system parameters such as β, M, and ρ on the optimal ϕ that maximizes the ergodic secrecy rate. The results in this subsection were generated based on the analytical expressions in (3.5), (3.7), and (3.15) for the SRCI data precoder, (3.19) for the CRCI data precoder, and (3.45) for the MF, SZF, and CZF data precoders.

Fig. 3.4 depicts the ergodic secrecy rate of the k^{th} MT in the n^{th} cell for the selfish data precoders SRCI, SZF, and MF as a function of the power allocation factor ϕ. All curves are concave and have a single maximum. For $\phi = 0$ only AN is transmitted, hence $R_{nk}^{\text{sec}} = 0$ results since no data can be transmitted. For $\phi = 1$, no AN is transmitted, hence $R_{nk}^{\text{sec}} = 0$ results since the capacity of the eavesdropper becomes unbounded (recall that we make the worst-case assumption that the eavesdropper can receive noise-free). For $0 < \phi < 1$, a positive secrecy rate may result depending on the system parameters and the precoding schemes. Since we keep the total transmit power fixed, the transmit power per MT decreases with increasing β. To compensate for this effect, the portion of the total transmit power allocated to data transmission should increase. This is confirmed by Fig. 3.4 where the optimal value of ϕ for $\beta = 0.5$ is larger than that for $\beta = 0.1$. Furthermore, for a given β, the optimal ϕ is the larger, the better the performance of the adopted data precoder is, i.e., for a more effective data precoder, transmitting the data signal with higher power is more beneficial, whereas for a less effective data precoder impairing the eavesdropper with a higher AN power is more beneficial.

In Fig. 3.5, we show the ergodic secrecy rate vs. ϕ for the CRCI, CZF, and SZF precoders. Similar to our observations in Fig. 3.4, for given system parameters, the optimal ϕ tends to be larger for more effective precoders that achieve a better performance. For the system with $M = 7, \rho = 0.1$, this can be observed by comparing the optimal ϕ for the SZF and CZF precoders. Furthermore, while for the pilot contamination free system with $M = 2, \rho = 0.3$, collaborative precoding is always preferable, for $M = 7, \rho = 0.1$, SZF precoding outperforms CZF and CRCI precoding for most considered values of ϕ, as in this scenario, suppressing the interference and AN leakage to the $\xi K = 20$ MTs in other cells with the available $N_T = 100$ antennas is not worth at the expense of sacrificing extra spatial degrees of freedom for collaborative designs. In particular, from (3.42), we obtain $K_{\text{CZF}>\text{SZF}} \leq 6$ for

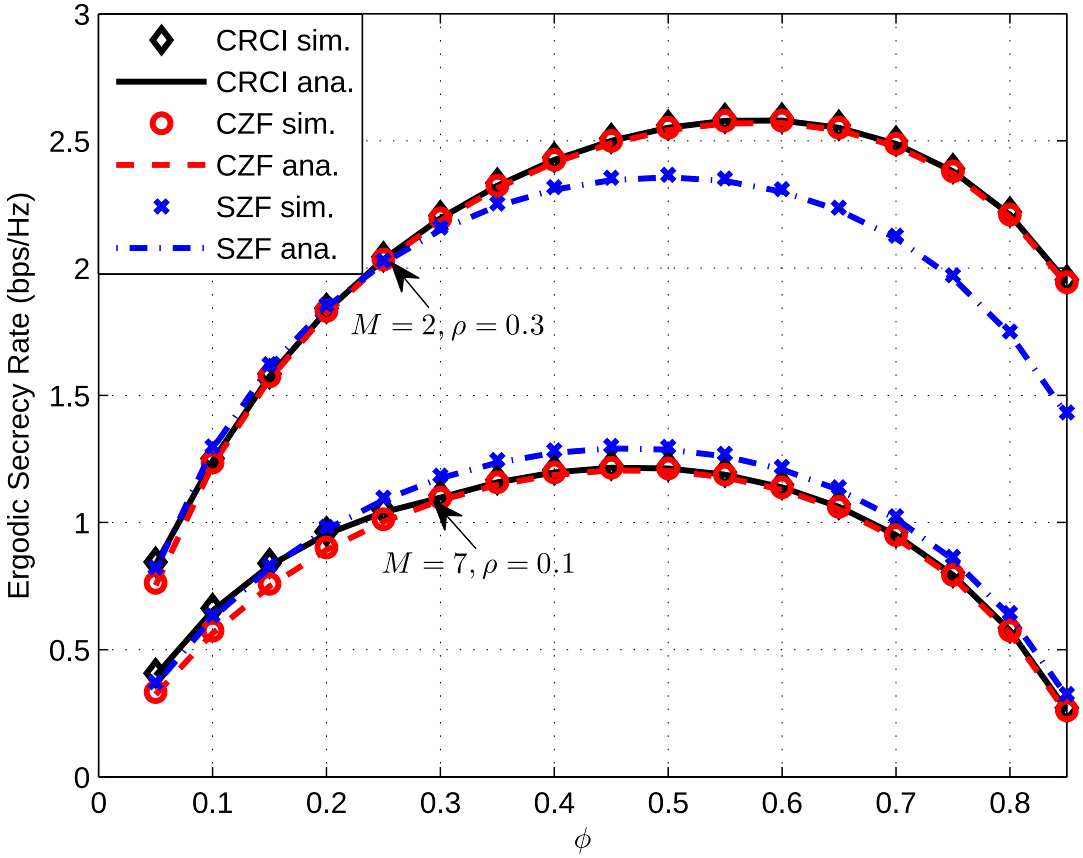

Figure 3.5: Ergodic secrecy rate vs. ϕ for different data precoders for a network with $P_T = 10$ dB, $N_T = 100$, $\xi = 2$, $p_\tau = P_T/\tau$, $\alpha = 0.1$, and $\beta = 0.1$.

$M = 7, \rho = 0.1$ and $K_{\text{CZF>SZF}} \leq 30$ for $M = 2, \rho = 0.3$, which confirms the results shown in Fig. 3.5.

Fig. 3.6 depicts the ergodic secrecy rate vs. ϕ for the considered conventional AN precoder structures. We consider a lightly loaded network with $\beta = 0.1$ and a moderately loaded network with $\beta = 0.4$. For $\beta = 0.1$, the CNS AN precoder outperforms the SNS AN precoder since, in this case, for the CNS AN precoder, the negative impact of having (slightly) fewer dimensions available for degrading the eavesdropper's channel (smaller value of L) is outweighed by the positive impact of causing less AN leakage (smaller value of $\tilde{Q}$). On the other hand, for $\beta = 0.4$, the

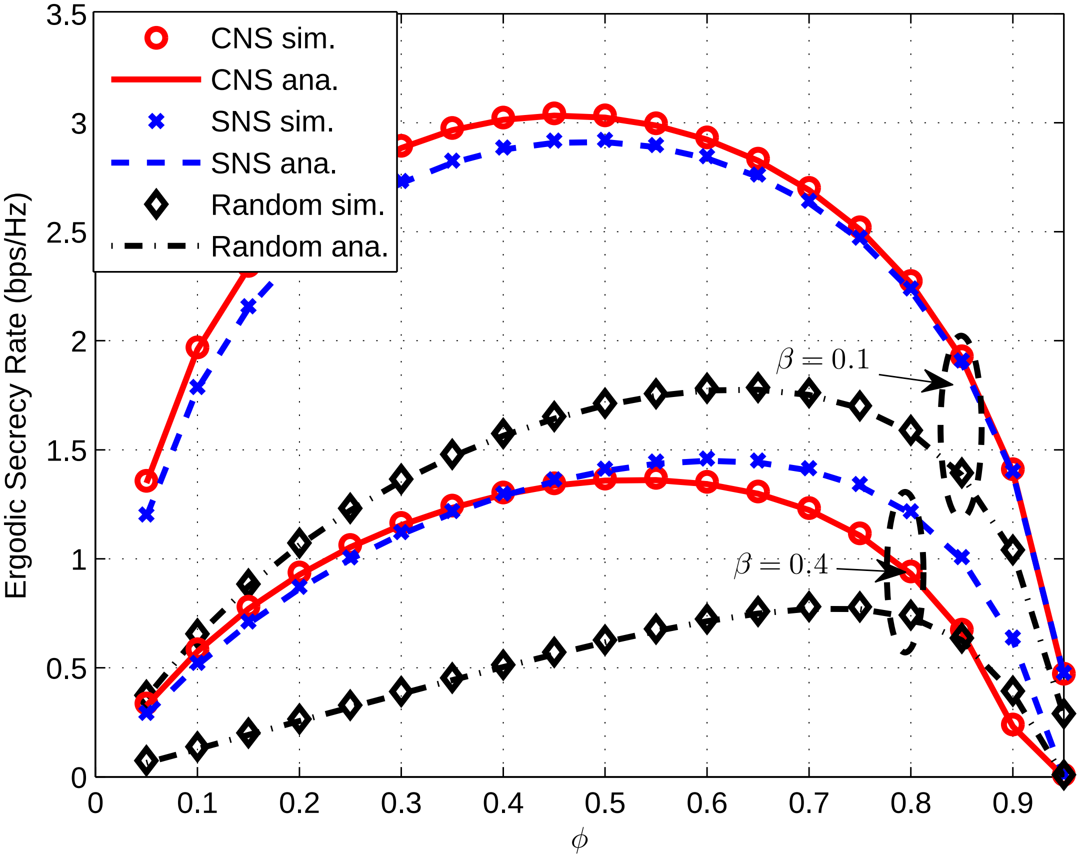

Figure 3.6: Ergodic secrecy rate vs. ϕ for different AN precoders for a network with $P_T = 10$ dB, $N_T = 100$, $\xi = 2$, $p_\tau = P_T/\tau$, $M = 2$, $\rho = 0.1$, and $\alpha = 0.1$.

CNS AN precoder has a substantially smaller L than the SNS precoder which cannot be compensated by its larger $\tilde{Q}$. Despite having the largest value of L, the random AN precoder has the worst performance for both considered cases because of its large AN leakage.

3.6.4 Conditions for Non-Zero Secrecy Rate

In Section 3.5.3, we showed that a positive ergodic secrecy rate is possible only if $\alpha < \alpha_s$. In Fig. 3.7, using (3.46), we plot α_s as a function of β. In the left hand side subfigure, we compare MF, SZF, and CZF data precoding for SNS AN precoding, and

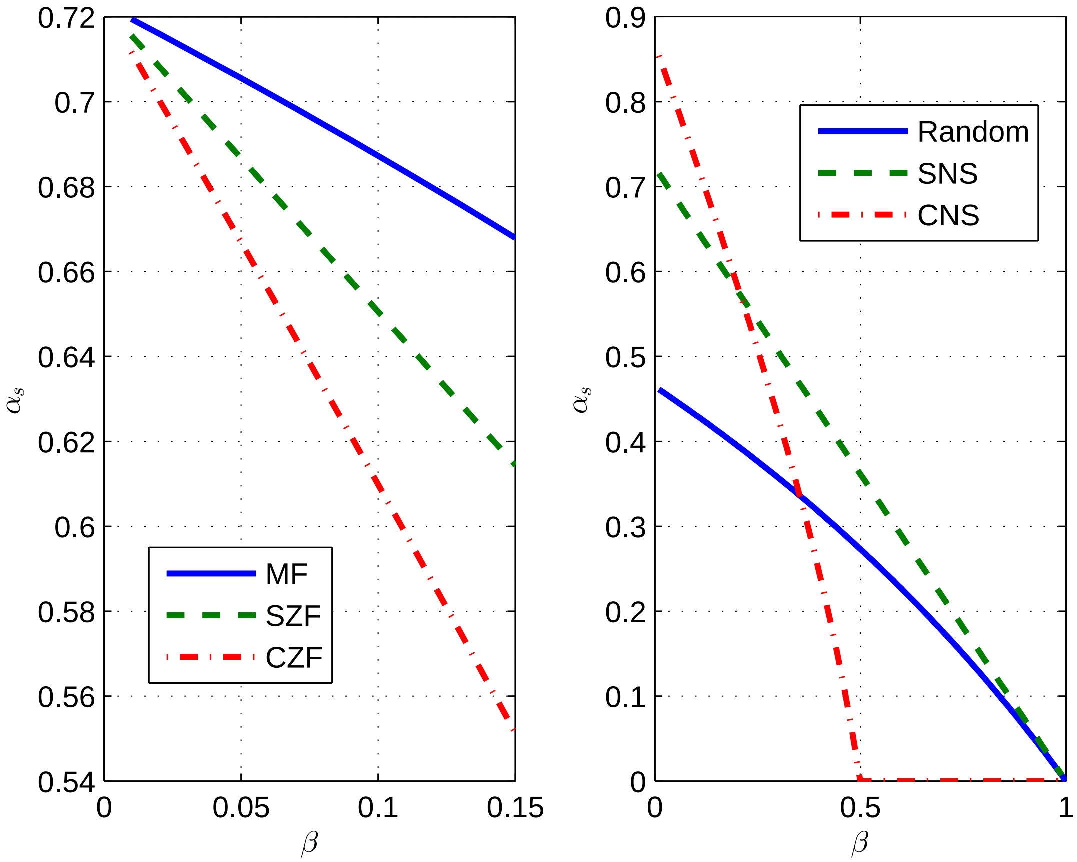

Figure 3.7: α_s vs. β for different data and AN precoders for a network with $P_T = 10$ dB, $N_T = 100$, $\xi = 2$, $p_\tau = P_T/\tau$, $\rho = 0.3$, and $M = 2$.

in the right hand side subfigure, we compare random, SNS, and CNS AN precoding for SZF data precoding. The comparison of the data precoders reveals that although SZF and CZF entail a much higher complexity, MF precoding achieves a larger α_s. Therefore, if the eavesdropper has a large number of antennas and small ergodic secrecy rates are targeted, simple MF precoding is always preferable. On the other hand, whether SNS or CNS AN precoder is preferable depends on the system load. For small values of β, CNS AN precoding can tolerate more eavesdropper antennas, whereas for large values of β, SNS AN precoding is preferable. Random AN precoding is outperformed by SNS and/or CNS AN preceding for any value of β. A closer examination of (3.46) reveals that this is always true if S/CZF data precoders are employed. However, for the MF data precoder, there are parameter combination for which random AN precoding outperforms SNS and CNS AN precoding.

3.6.5 Low-Complexity POLY Data and AN Precoders

In this subsection, we evaluate the ergodic secrecy rates of the proposed low-complexity POLY data and AN precoders. To this end, we consider again a lightly loaded network with little inter-cell interference ($M = 2$, $\beta = 0.1$, $\rho = 0.1$) and a dense network with more inter-cell interference ($M = 7$, $\beta = 0.15$, $\rho = 0.3$). All results shown in this section were obtained by simulation. For each simulation point, the optimal value of ϕ was found numerically and applied. In Figs. 3.8 and 3.9, we show the ergodic secrecy rate of the k^{th} MT in the n^{th} cell as a function of the pilot energy, τp_τ. As expected, for all considered schemes, the ergodic secrecy rate is monotonically increasing in the pilot energy since more accurate channel estimates improve performance and the total power used for data and AN transmission, P_T, is assumed to be fixed.

In Fig. 3.8, we depict the ergodic secrecy rates for the proposed POLY data precoder for different values of $\mathcal{I}$ and compare them to those of conventional selfish data precoders. For the sake of comparison, all data precoders are combined with the SNS AN precoder. As the number of terms of the polynomial $\mathcal{I}$ increase, the performance of the POLY data precoder quickly improves and approaches that of the SRCI data precoder. The convergence is faster for the dense network considered in the right hand side subfigure, where the performance difference between all precoders is smaller in general since interference cannot be as efficiently avoided as for the lightly loaded network.

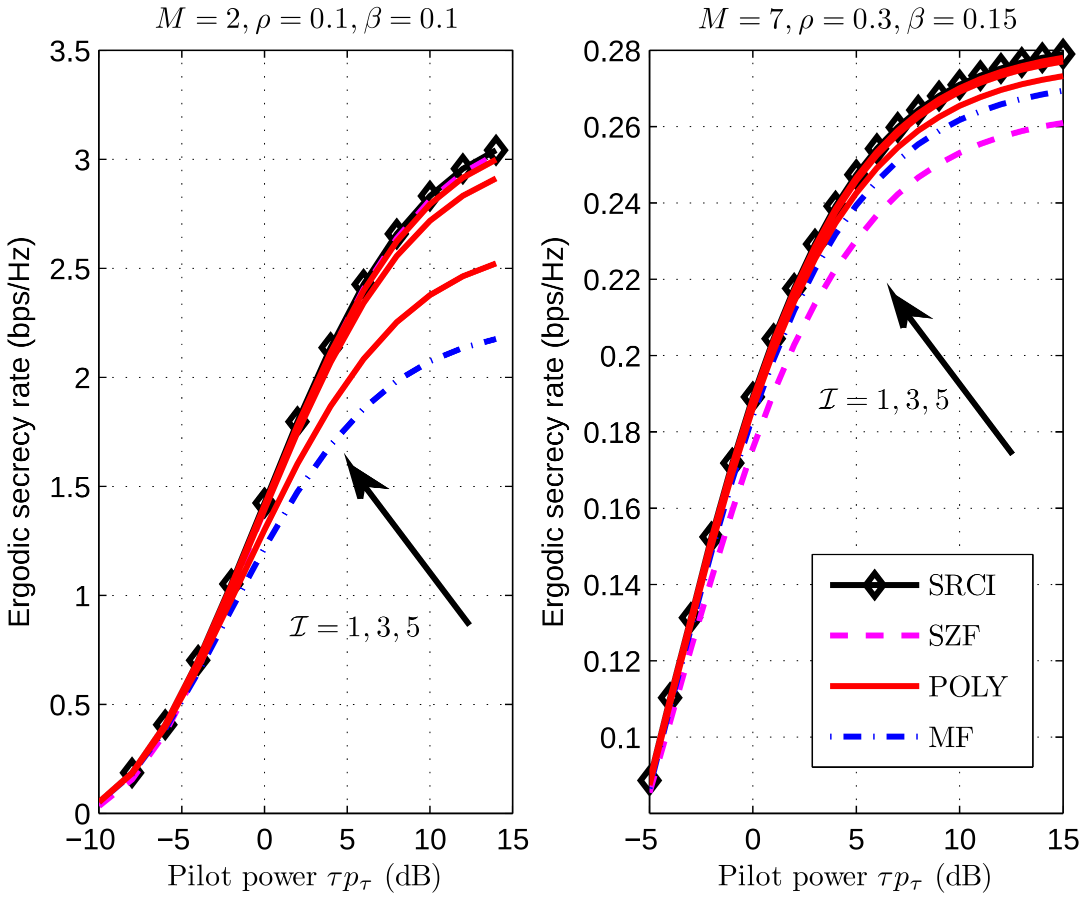

Figure 3.8: Ergodic secrecy rate for POLY and conventional selfish data precoders for a network employing the optimal ϕ, $P_T = 10$ dB, $\xi = 1$, $p_\tau = P_T/\tau$, $N_T = 200$, and $\alpha = 0.1$.

In Fig. 3.9, we show the ergodic secrecy rates for the proposed POLY AN precoder for different values of $\mathcal{J}$ and compare them to those of the random and SNS AN precoders. For the sake of comparison, all AN precoders are combined with SZF data precoding. The POLY AN precoder quickly approaches the performance of the SNS AN precoder as the polynomial order $\mathcal{J}$ increases. Similar to the POLY data precoders, the convergence is faster for the dense network where the performance differences between different AN precoders are also smaller. For the denser network, even the random AN precoder is a viable option and suffers only from a small loss in performance compared to the SNS AN precoder.

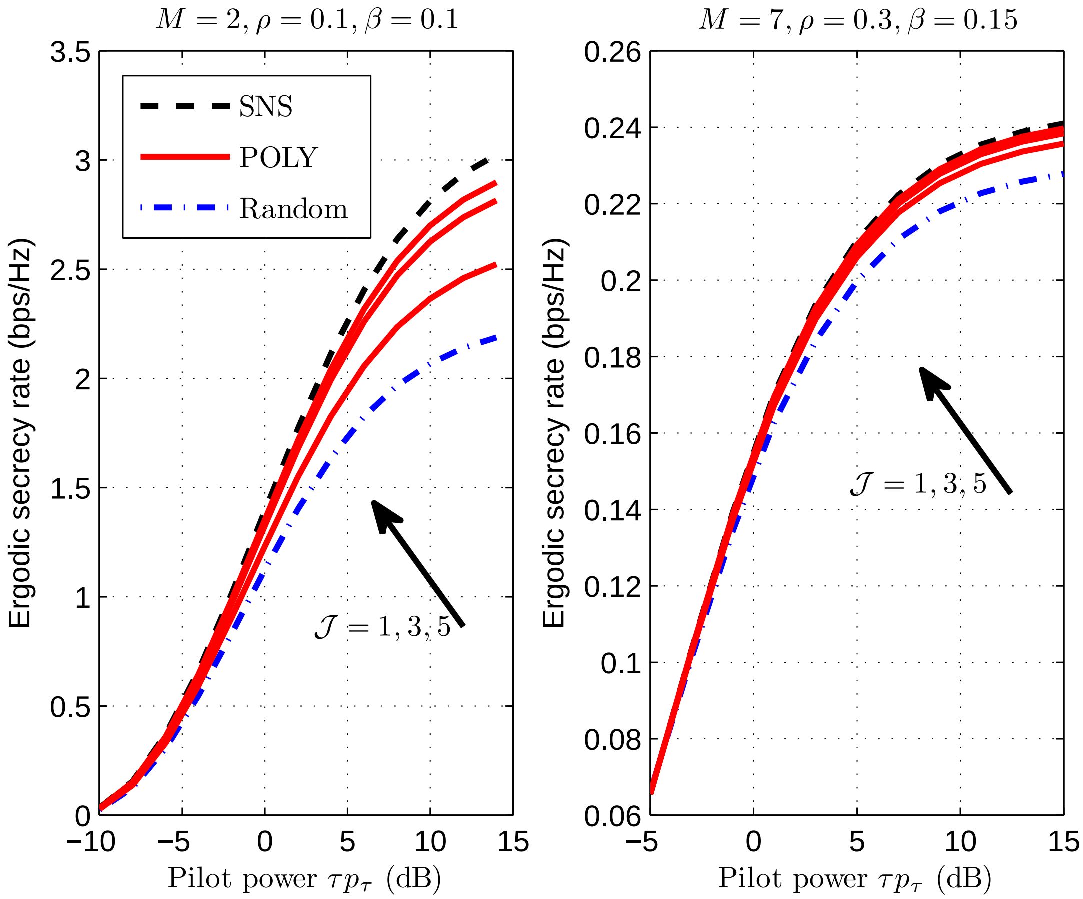

Figure 3.9: Ergodic secrecy rate for POLY and SNS AN precoders for a network employing the optimal ϕ, $P_T = 10$ dB, $\xi = 1$, $p_\tau = P_T/\tau$, $N_T = 200$, and $\alpha = 0.1$.

3.6.6 Complexity-Performance Tradeoff

In this subsection, we investigate the tradeoff between the ergodic secrecy rate performance and the computational complexity for the proposed data and AN precoders in Figs. 3.10 and 3.11, respectively. In particular, Figs. 3.10 and 3.11 depict the ergodic secrecy rate on the right hand side and the computational complexity (in Giga FLOP) on the left hand side, both as a function of the numbers of users in a cell. For the considered setting, the performance gains of collaborative data and AN precoding compared to selfish strategies are moderate, but the associated increase in complexity is substantial, especially for large K.

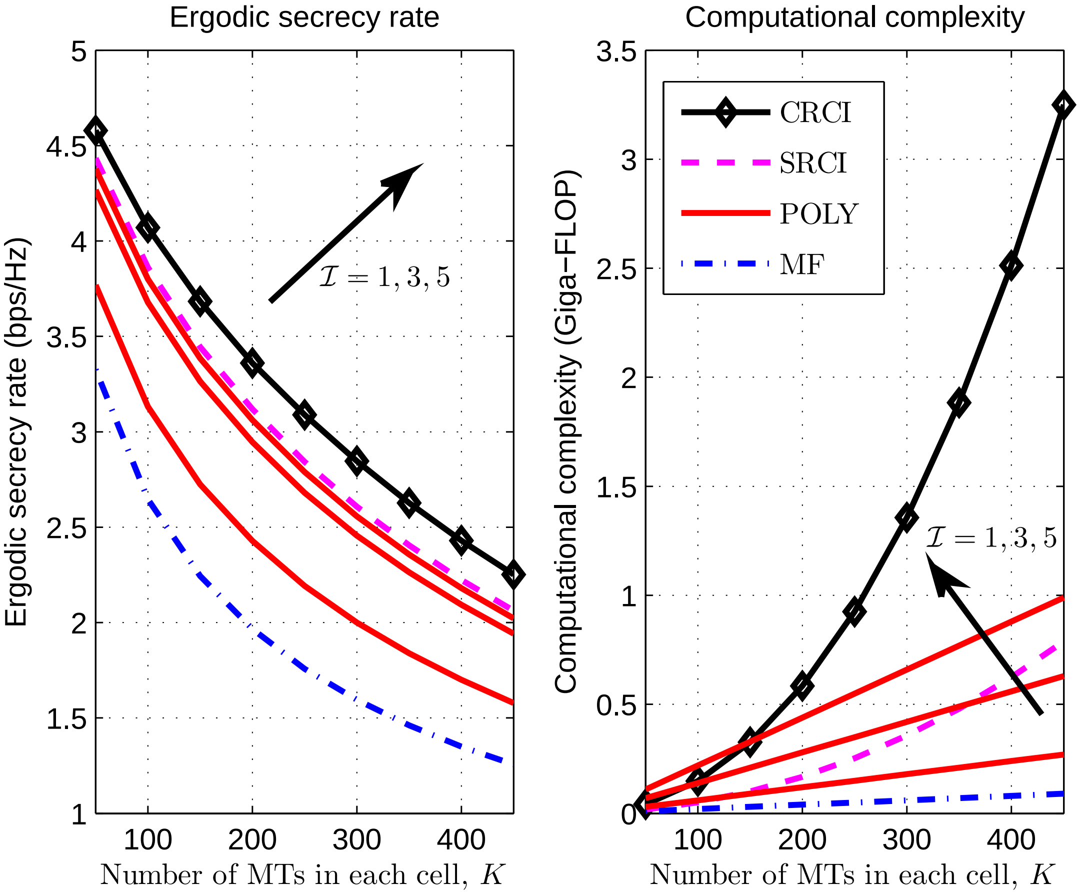

Figure 3.10: Ergodic secrecy rate (left hand side) and computational complexity (right hand side) of various linear data precoders for a network employing $P_T = 10$dB, $N_T = 1000$, $p_\tau = P_T/\tau$, $M = \xi = 2$, $\rho = 0.1$, $T - \tau = 100$, and an SNS AN precoder.

Fig. 3.10 illustrates that for the considered setting a POLY data precoder with $\mathcal{I} = 1$ achieves a better performance than the MF precoder but has substantially lower complexity than the SRCI precoder. For large $\mathcal{I}$, the POLY data precoder has a lower complexity than the SRCI precoder for large K. However, even for small K, the POLY precoder may be preferable as it does not incur the stability issues that may arise in the implementation of the large-scale matrix inversions required for the SRCI precoder.

Fig. 3.11 shows that for the considered setting the proposed POLY AN precoder with $\mathcal{J} = 1$ outperforms the Random AN precoder, and with $\mathcal{J} = 5$ achieves al-

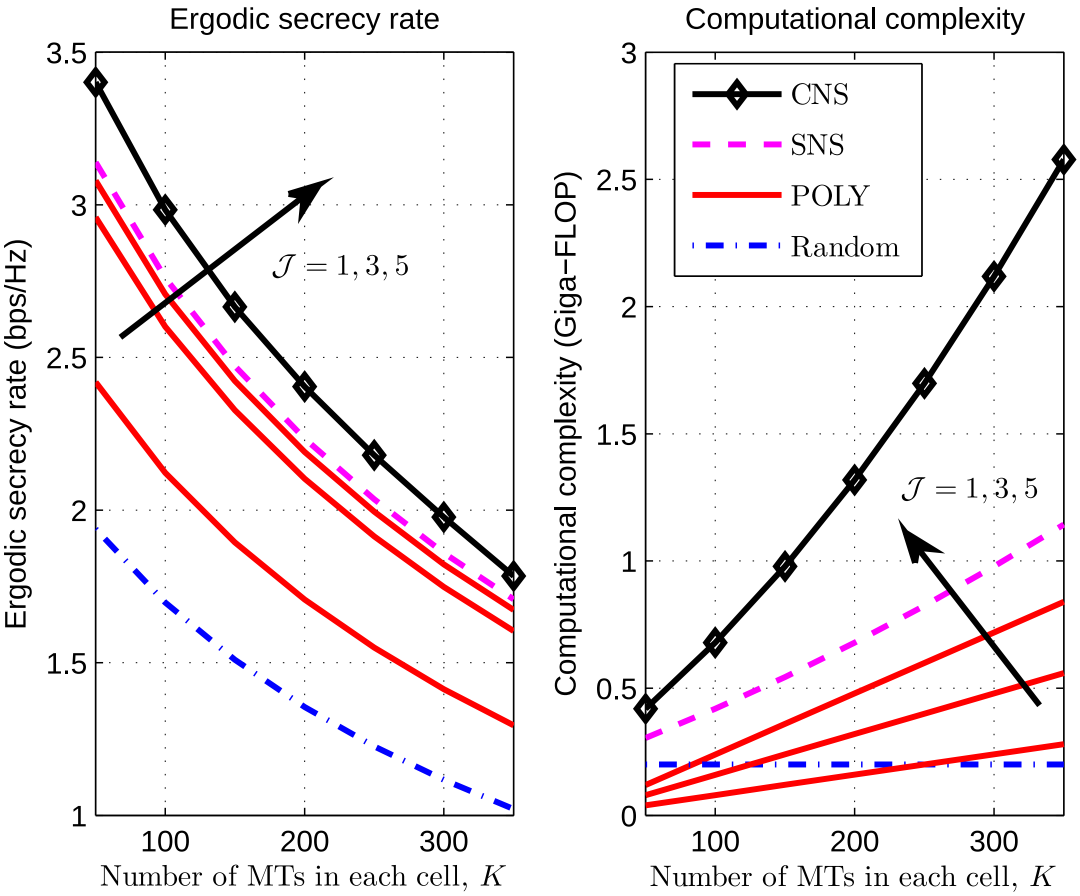

Figure 3.11: Ergodic secrecy rate (left hand side) and computational complexity (right hand side) of various linear AN precoders for a network employing $P_T = 10$dB, $N_T = 1000$, $p_\tau = P_T/\tau$, $M = \xi = 2$, $\rho = 0.1$, $T - \tau = 100$, and an SZF data precoder.

most the same performance as the SNS AN precoder but with a substantially lower complexity. We further observe that for small K, the proposed POLY AN precoder requires even lower complexity than the Random AN precoder, owing to the efficient structure given in (3.35) operated by Horner's rule.

3.7 Conclusions

In this chapter, we considered downlink multi-cell massive MIMO systems employing linear data and AN precoding for physical layer security provisioning. We analyzed and compared the achievable ergodic secrecy rate of various conventional data and AN precoders in the presence of pilot contamination. To this end, we also optimized the regularization constants of the selfish and collaborative RCI precoders in the presence of AN and multi-cell interference. In addition, we derived linear POLY data and AN precoders which offer a good compromise between complexity and performance in massive MIMO systems. Interesting findings of this chapter include: 1) Collaborative data precoders outperform selfish designs only in lightly loaded systems where a sufficient number of degrees of freedom for suppressing inter-cell interference and sufficient resources for training are available. 2) Similarly, CNS AN precoding is preferable over SNS AN precoding in lightly loaded systems as it causes less AN leakage to the information-carrying signal, whereas in more heavily loaded systems, CNS AN precoding does not have sufficient degrees of freedom for effectively degrading the eavesdropper channel and SNS AN precoding is preferable. 3) For a large number of eavesdropper antennas, where only small positive secrecy rates are achievable, MF data precoding is always preferable compared to SZF and CZF data precoding. 4) The proposed POLY data and AN precoders approach the performances of the SRCI data and SNS AN precoders with only a few terms in the respective matrix polynomials and are attractive options for practical implementation.

Chapter 4

Hardware Impairments in Secure Massive MIMO Systems

4.1 Introduction

Since security is a critical concern for future communication systems, facilitating secrecy at the physical layer of massive MIMO systems has received significant attention recently. All aforementioned works on secure massive MIMO systems including Chapters 2 and 3 are based on the assumption that the transceivers of the legitimate users are equipped with perfect hardware components, i.e., the effects of hardware impairments were not taken into account. Nevertheless, all practical implementations do suffer from hardware impairments such as phase noise, quantization errors, amplification noise, and nonlinearities [18]. These impairments are expected to be particularly pronounced in massive MIMO systems as the excessive number of BS antennas makes the use of low-cost components desirable to keep the overall capital expenditures for operators manageable. Although hardware impairments can be mitigated by analog and digital signal processing techniques [19], they cannot be removed completely, due to the randomness introduced by the different sources of imperfection. The remaining residual hardware impairments can be modelled by a combination of phase noise and additive distortion noises at the transmitter and the receiver [19]. Several works have investigated the impact of hardware impairments on massive MIMO systems [18], [20, 21, 22]. They all demonstrated that hardware impairments can severely limit the performance of massive MIMO systems. Thereby, a crucial role is played by the degradation caused by phase noise to the quality of the CSI estimates needed for precoder design. On the one hand, phase noise causes the CSI estimates to become outdated more quickly, and on the other hand, it may cause a loss of orthogonality of the pilot sequences employed by the different users in a cell for uplink training. To overcome the latter effect, so-called TO and SO pilot sequences were investigated in [22]. Furthermore, the impact of the number of LOs employed at the massive MIMO BS on the performance in the presence of phase noise was studied in [20, 22].

All aforementioned works [18], [20, 21, 22] studied the impact of hardware impairments in the context of conventional massive MIMO system design without regard for communication secrecy. However, if communication secrecy is considered, an additional challenge arises: Whereas the legitimate user of the system will likely employ low-cost equipment giving rise to hardware impairments, the eavesdropper is expected to employ high-quality equipment which can compensate for all hardware impairments except for the additive distortion noise at the BS. This disparity in equipment quality was not considered in the related work on physical layer security [43]-[64] nor in the related work on hardware impairments [18], [20, 21, 22] and necessitates the development of a new analysis and design framework. For example, NS AN precoding, which was widely used to enhance the achievable secrecy rate of massive MIMO systems [25, 43, 64], becomes ineffective in the presence of phase noise.

Motivated by the above considerations, in this chapter, we present the first study of physical layer security in hardware constrained massive MIMO systems. Thereby, we focus on the downlink and adopt for the legitimate links the generic residual hardware impairment model from [19, 22], which includes the effects of multiplicative phase noise and additive distortion noise at the BS and the users. As a worst-case scenario, the eavesdropper is assumed to employ ideal hardware. Our main contributions are summarized as follows.

- For the adopted generic residual hardware impairment model, we derive a tight lower bound for the ergodic secrecy rate achieved by a downlink user when MF data precoding is employed at the massive MIMO BS. The derived bound provides insight into the impact of various system and channel parameters, such as the phase noise variance, the additive distortion noise parameters, the AN precoder design, the amount of power allocated to the AN, the pilot sequence design, the number of deployed LOs, and the number of users, on the ergodic secrecy rate.

- As conventional NS AN precoding is sensitive to phase noise, we propose a novel G-NS AN precoding design, which mitigates the AN leakage caused to the legitimate user in the presence of phase noise at the expense of a reduction of the available spatial degrees of freedom. The proposed method leads to significant performance gains, especially in systems with large numbers of antennas at the BS.

- We generalize the SO and TO pilot sequence designs from [22] to orthogonal pilot sequences with arbitrary numbers of non-zero elements. Although SO sequences, which have no zero elements, are preferable for small phase noise variances, sequence designs with zero elements become beneficial in the presence of strong phase noise.

- Our analytical and numerical results reveal that while hardware impairments in general degrade the achievable secrecy rate, the proposed countermeasures are effective in limiting this degradation. Furthermore, surprisingly, there are cases when the additive distortion noise at the BS is beneficial for the secrecy performance as it can have a similar effect as AN.

The remainder of this chapter is organized as follows. In Section 4.2, the models for uplink training and downlink data transmission in the considered massive MIMO system with imperfect hardware are presented. In Section 4.3, we derive a lower bound on achievable ergodic secrecy rate and introduce the proposed G-NS AN precoder design. The impact of the various system and channel parameters on the secrecy performance is investigated based on the derived lower bound in Section 4.4. In Section 4.5, the achievable secrecy rate is studied via simulation and numerical results, and conclusions are drawn in Section 4.6.

4.2 System and Channel Models

The considered massive MIMO system model comprises an N-antenna BS, K single-antenna MTs, and an N_E-antenna eavesdropper. The eavesdropper is passive in order to hide its existence from the BS and the MTs. Similar to [18, 22], we assume that after proper compensation the residual hardware impairments manifest themselves at the BS and the MTs in the form of 1) multiplicative phase noises at transmitter and receiver, 2) transmit and receive power dependent distortion noises at transmitter and receiver, respectively, and 3) amplified thermal noise at the receiver. The impact of this general hardware impairment model on uplink training and downlink data transmission is investigated in Sections 4.2.1 and 4.2.2, respectively, and the signal model for the eavesdropper is presented in Section 4.2.3.

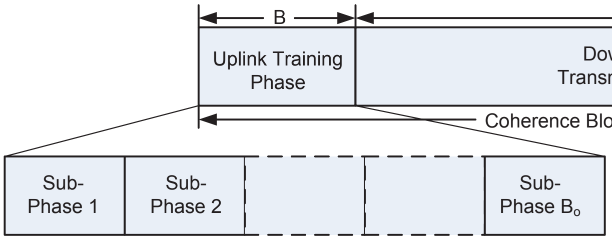

Figure 4.1: Uplink training and downlink transmission phase.

4.2.1 Uplink Pilot Training under Hardware Impairments

In massive MIMO systems, the CSI is usually acquired via uplink training by exploiting the channel reciprocity between uplink and downlink [5, 8]. Here, we assume that the first B symbol intervals of the coherence time, which comprises T symbol intervals, are used for uplink training. Thereby, we split the training phase into B_o sub-phases of lengths B_b, $1 \leq b \leq B_o$, where $\sum_{b=1}^{B_o} B_b = B$, cf. Fig. 4.1. Furthermore, the K MTs are assigned to B_o disjunct sets $\mathcal{S}_b$, $1 \leq b \leq B_o$, with $|\mathcal{S}_b| \leq B_b$ and $\sum_{b=1}^{B_o} |\mathcal{S}_b| = K$. In training sub-phase b, the MTs in set $\mathcal{S}_b$ emit mutually orthogonal pilot sequences $\boldsymbol{\omega}_k = [\omega_k(1), \omega_k(2), \ldots, \omega_k(B_b)]^T \in \mathbb{C}^{B_b \times 1}, k \in \mathcal{S}_b$, for which we assume a per-pilot power constraint $|\omega_k(t)|^2 = p_\tau, \forall k, t$, whereas all MTs $k \notin \mathcal{S}_b$ are silent. For larger values of B_b, the total energy of the pilot sequences is larger but, as will be shown later, the loss of orthogonality caused by phase noise becomes also more pronounced. Hence, B_b or equivalently B_o (assuming a fixed B) should be optimized for maximization of the secrecy rate. We note that the proposed pilot design is a generalization of the SO and TO pilot designs proposed in [22, 20] which result as special cases for $B_o = 1$ and $B_o = B$, respectively.

In symbol interval $t \in \mathcal{T}_b$, where $\mathcal{T}_b$ denotes the set of symbol intervals in training sub-phase b, $1 \leq b \leq B_o$, the received uplink vector $\mathbf{y}^{\mathrm{UL}}(t) \in \mathbb{C}^{N \times 1}$ at the BS is given by

$$\mathbf{y}^{\mathrm{UL}}(t) = \sum_{k\in\mathcal{S}_b} \mathbf{\Theta}_k(t)\mathbf{g}_k(\omega_k(t) + \eta_{t,k}^{\mathrm{MT}}(t)) + \boldsymbol{\eta}_r^{\mathrm{BS}}(t) + \boldsymbol{\xi}^{\mathrm{UL}}(t). \tag{4.1}$$

Here, the channel vector of the k^{th} MT, $\mathbf{g}_k \sim \mathbb{CN}(\mathbf{0}_N, \beta_k \mathbf{I}_N)$, is modelled as block Rayleigh fading, where β_k denotes the path-loss. Thereby, $\mathbf{g}_k$ is assumed to be constant during coherence time T and change independently afterwards. In (4.1), the terms $\mathbf{\Theta}_k(t)$, $\eta_{t,k}^{\mathrm{MT}}(t)$, $\boldsymbol{\eta}_r^{\mathrm{BS}}(t)$, and $\boldsymbol{\xi}^{\mathrm{UL}}(t)$ characterize the hardware impairments affecting the uplink training phase and are explained in detail in the following:

1) Phase noise: Matrix

$$\mathbf{\Theta}_k(t) = \mathrm{diag}\left(e^{j\theta_k^1(t)}\mathbf{1}_{1\times N/N_o}, \ldots, e^{j\theta_k^{N_o}(t)}\mathbf{1}_{1\times N/N_o}\right) \in \mathbb{C}^{N\times N} \tag{4.2}$$

models the phase noise originating from the free-running LOs equipped at the BS and the MTs [20]. Thereby, we assume that at the BS each group of $N/N_o \in \mathbb{Z}$ antennas is connected to one free-running LO. $\theta_k^l(t) = \psi_l(t) + \phi_k(t)$ is the phase noise that distorts the link between the l^{th} LO at the BS and the k^{th} MT. Adopting the discrete-time Wiener phase noise model [20], in time interval t, the phase noises at the l^{th} LO of the BS and the k^{th} MT are modelled as $\psi_l(t) \sim \mathbb{CN}(\psi_l(t-1), \sigma_\psi^2)$, $1 \le l \le N_o$, and $\phi_k(t) \sim \mathbb{CN}(\phi_k(t-1), \sigma_\phi^2)$, $1 \le k \le K$, where σ_ψ^2 and σ_ϕ^2 are the phase noise (increment) variances at the BS and the MTs, respectively.

2) Distortion noise: $\eta_{t,k}^{\mathrm{MT}}(t) \in \mathbb{C}$ and $\boldsymbol{\eta}_r^{\mathrm{BS}}(t) \in \mathbb{C}^{N\times 1}$ model the additive distortion noise at the k^{th} MT and the BS, respectively, which originates from the residual effects after compensation of hardware impairments such as power amplifier non-linearities at the transmitter, quantization noise in the analog-to-digital converters (ADCs) at the receiver, etc. [18]. Distortion noise is modeled as a Gaussian distributed random process in the literature [18, 19]. This model has been experimentally verified in

[76]. Furthermore, at each antenna, the distortion noise power is proportional to the corresponding signal power, i.e., $\eta_{t,k}^{\mathrm{MT}}(t) \sim \mathbb{CN}(0, \upsilon_{t,k}^{\mathrm{MT}})$ and $\boldsymbol{\eta}_r^{\mathrm{BS}}(t) \sim \mathbb{CN}(\mathbf{0}_N, \boldsymbol{\Upsilon}_r^{\mathrm{BS}})$, where

$$\upsilon_{t,k}^{\mathrm{MT}} = \kappa_t^{\mathrm{MT}} \mathbb{E}[|\omega_k(t)|^2] \quad \text{and} \quad \boldsymbol{\Upsilon}_r^{\mathrm{BS}} = \kappa_r^{\mathrm{BS}} \sum_{k=1}^{K} \mathbb{E}[|\omega_k(t)|^2] \mathbf{R}_k^{\mathrm{diag}}. \tag{4.3}$$

Here, $\mathbf{R}_k^{\mathrm{diag}} = \operatorname{diag}\left(|g_k^1|^2, \ldots, |g_k^N|^2\right)$, where g_k^i denotes the i^{th} element of $\mathbf{g}_k$, and parameters $\kappa_t^{\mathrm{MT}}, \kappa_r^{\mathrm{BS}} > 0$ denote the ratio between the additive distortion noise variance and the signal power and are measures for the severity of the residual hardware impairments.

3) Amplified thermal noise: $\boldsymbol{\xi}^{\mathrm{UL}}(t) \sim \mathbb{CN}(\mathbf{0}_N, \xi^{\mathrm{UL}} \mathbf{I}_N)$ models the thermal noise amplified by the low noise amplifier and other components such as mixers at the receiver [22]. Therefore, the variance of this noise is generally larger than that of the actual thermal noise σ_n^2, i.e., $\xi^{\mathrm{UL}} > \sigma_n^2$.

For channel estimation, we collect the signal vectors received during the b^{th} training phase in vector $\boldsymbol{\psi}_b = [(\mathbf{y}^{\mathrm{UL}}(\overline{B}_{b-1}+1))^T, \ldots, (\mathbf{y}^{\mathrm{UL}}(\overline{B}_b))^T]^T \in \mathbb{C}^{B_b N \times 1}$, $b = 1, \ldots, B_o$, where $\overline{B}_b \triangleq \sum_{i=1}^{b} B_i$ and $\overline{B}_0 = 0$, and define the effective channel vector at time t as $\mathbf{g}_k(t) = \boldsymbol{\Theta}_k(t)\mathbf{g}_k$. With these definitions, the MMSE estimate of the channel of MT $k \in \mathcal{S}_b$ at time $t \in \{B+1, \ldots, T\}$ (i.e., during the data transmission phase) can be written as [22]

$$\hat{\mathbf{g}}_k(t) = \mathbb{E}[\mathbf{g}_k(t)\boldsymbol{\psi}_b^H] \left(\mathbb{E}[\boldsymbol{\psi}_b\boldsymbol{\psi}_b^H]\right)^{-1} \boldsymbol{\psi}_b = \left(\beta_k \boldsymbol{\omega}_k^H \boldsymbol{\Theta}_{\sigma(t)}^b \boldsymbol{\Sigma}_b^{-1} \otimes \mathbf{I}_N\right) \boldsymbol{\psi}_b, \tag{4.4}$$

where

$$\boldsymbol{\Theta}_{\sigma(t)}^b = \operatorname{diag}\left(e^{-\frac{\sigma_\psi^2+\sigma_\phi^2}{2}|t-\overline{B}_{b-1}-1|}, \ldots, e^{-\frac{\sigma_\psi^2+\sigma_\phi^2}{2}|t-\overline{B}_b|}\right) \tag{4.5}$$

and

$$\boldsymbol{\Sigma}_b = \sum_{k \in \mathcal{S}_b} \beta_k \left(\mathbf{W}_k^b + \mathbf{U}_k^b \right) + \xi^{\mathrm{UL}} \mathbf{I}_{B_b}. \tag{4.6}$$

Here, we adopted the definitions $[\mathbf{W}_k^b]_{i,j} = \omega_k(i)\omega_k^*(j) e^{-\frac{\sigma_\psi^2+\sigma_\phi^2}{2}|i-j|}$, $i, j \in \{1, \dots B_b\}$, and $\mathbf{U}_k^b = (\kappa_t^{\mathrm{MT}} + \kappa_r^{\mathrm{BS}}) p_\tau \mathbf{I}_{B_b}$.

Considering the properties of MMSE estimation, the channel can be decomposed as $\mathbf{g}_k(t) = \hat{\mathbf{g}}_k(t) + \mathbf{e}(t)$, $t = 1, \dots, B$, where $\hat{\mathbf{g}}_k(t)$ denotes the MMSE channel estimate given in (4.4) and $\mathbf{e}_k(t)$ represents the estimation error. $\hat{\mathbf{g}}_k(t)$ and $\mathbf{e}(t)$ are mutually uncorrelated and have zero mean [18, Theorem 1]. The error covariance matrix is given by

$$\mathbb{E}[\mathbf{e}_k(t)\mathbf{e}_k^H(t)] = \beta_k \left(1 - \beta_k \boldsymbol{\omega}_k^H \boldsymbol{\Theta}_{\sigma(t)}^b \boldsymbol{\Sigma}_b^{-1} \boldsymbol{\Theta}_{\sigma(t)}^b \boldsymbol{\omega}_k \right) \mathbf{I}_N. \tag{4.7}$$

Eqs. (4.4)-(4.7) reveal that for $|\mathcal{S}_b| > 1$ and $\sigma_\psi^2, \sigma_\phi^2 > 0$, the channel estimate of the k^{th} MT contains contributions from channels of other MTs emitting their pilots in the same training sub-phase, i.e., pilot contamination occurs although the emitted pilots are orthogonal. This loss of orthogonality at the receiver is introduced by the phase noise via matrices $\boldsymbol{\Theta}_{\sigma(t)}^b$ and $\mathbf{W}_k^b$, and can be avoided only by enforcing that in any sub-phase only one MT emits its pilots, i.e., $|\mathcal{S}_b| = 1$, $1 \leq b \leq B_o$. In particular, for the case $|\mathcal{S}_b| = B_b = 1$, $1 \leq b \leq B_o = B$, for symbol interval $t \in \{B+1, \dots T\}$, the MMSE channel estimate of MT $k \in \mathcal{S}_b$ can be simplified to

$$\hat{\mathbf{g}}_k(t) = \frac{\beta_k e^{-\frac{\sigma_\psi^2+\sigma_\phi^2}{2}|t-b|}}{p_\tau \beta_k (1 + \kappa_t^{\mathrm{MT}} + \kappa_r^{\mathrm{BS}}) + \xi^{\mathrm{UL}}} \mathbf{y}^{\mathrm{UL}}(b), \tag{4.8}$$

with $\mathbf{y}^{\mathrm{UL}}(t)$ given in (4.1), i.e., $\hat{\mathbf{g}}_k(t)$ is not affected by the channels of other MTs despite the phase noise. The corresponding error covariance matrix simplifies to

$$\mathbb{E}[\mathbf{e}(t)\mathbf{e}^H(t)] = \beta_k \left(1 - \frac{p_\tau \beta_k}{p_\tau \beta_k (1 + \kappa_t^{\mathrm{MT}} + \kappa_r^{\mathrm{BS}}) + \xi^{\mathrm{UL}}}\right) \mathbf{I}_N. \tag{4.9}$$

Eqs. (4.4) and (4.8) reveal that the channel estimate depends on time t. As a consequence, ideally, the channel-dependent data and AN precoders employed for downlink transmission should be recomputed for every symbol interval of the data transmission phase, which entails a high computational complexity. Therefore, in the following, we assume that data and AN precoders are computed based on the channel estimate for one symbol interval t_0 (e.g., $t_0 = B + 1$) and are then employed for precoding during the entire data transmission phase, i.e., for $t \in \{B+1, \ldots, T\}$. For notational conciseness, we denote the corresponding channel estimate by $\hat{\mathbf{g}}_k = \hat{\mathbf{g}}_k(t_0)$, $k = \{1, \ldots, K\}$.

4.2.2 Downlink Data Transmission and Linear Precoding

Assuming channel reciprocity, during the downlink data transmission phase, the received signal at the k^{th} MT in time interval $t \in \{B+1, \ldots, T\}$ is given by

$$y_k^{\mathrm{DL}}(t) = \mathbf{g}_k^H \mathbf{\Theta}_k^H(t)(\mathbf{x} + \boldsymbol{\eta}_t^{\mathrm{BS}}(t)) + \eta_{r,k}^{\mathrm{MT}}(t) + \xi_k^{\mathrm{DL}}(t). \tag{4.10}$$

In (4.10), similar to the uplink, $\boldsymbol{\eta}_t^{\mathrm{BS}}(t) \sim \mathbb{CN}(\mathbf{0}_N, \mathbf{\Upsilon}_t^{\mathrm{BS}})$ and $\eta_{r,k}^{\mathrm{MT}}(t) \sim \mathbb{CN}(0, \upsilon_{r,k}^{\mathrm{MT}}(t))$ denote the downlink distortion noise [18] at the BS and the k^{th} MT, respectively, where

$$\mathbf{\Upsilon}_t^{\mathrm{BS}} = \kappa_t^{\mathrm{BS}} \mathrm{diag}\left(X_{11}, \ldots, X_{NN}\right) \quad \text{and} \quad \upsilon_{r,k}^{\mathrm{MT}}(t) = \kappa_r^{\mathrm{MT}} \mathbf{g}_k^H(t) \mathbf{X} \mathbf{g}_k(t) \tag{4.11}$$

with $\mathbf{X} = \mathbb{E}[\mathbf{x}\mathbf{x}^H]$ and $X_{ii} = [\mathbf{X}]_{ii}, i = 1, \ldots, N$. Furthermore, $\xi_k^{\mathrm{DL}}(t) \sim \mathbb{CN}(0, \xi^{\mathrm{DL}})$ represents the amplified thermal noise at the k^{th} MT. For simplicity of presentation, we assume that parameters κ_t^{BS}, κ_r^{MT}, and ξ^{DL} are identical for all MTs.

The downlink transmit signal $\mathbf{x} \in \mathbb{C}^{N\times 1}$ in (4.10) is modeled as

$$\mathbf{x} = \sqrt{p}\mathbf{F}\mathbf{s} + \sqrt{q}\mathbf{A}\mathbf{z} \in \mathbb{C}^{N\times 1}, \tag{4.12}$$

where the data symbol vector $\mathbf{s} \in \mathbb{C}^{K\times 1}$ and the AN vector $\mathbf{z} \in \mathbb{C}^{L\times 1}$, $L \leq N$, are multiplied by data precoder $\mathbf{F} \in \mathbb{C}^{N\times K}$ and AN precoder $\mathbf{A} \in \mathbb{C}^{N\times L}$, respectively. As we assume that the eavesdropper's CSI is not available at the BS, AN is injected to degrade the eavesdropper's ability to decode the data intended for the MTs [25, 43, 64]. Thereby, it is assumed that the components of $\mathbf{s}$ and $\mathbf{z}$ are independent and identically distributed (i.i.d.) circularly symmetric complex Gaussian (CSCG) random variables, i.e., $\mathbf{s} \sim \mathbb{CN}(\mathbf{0}_K, \mathbf{I}_K)$ and $\mathbf{z} \sim \mathbb{CN}(\mathbf{0}_L, \mathbf{I}_L)$. In (4.12), $p = \phi P_T/K$ and $q = (1-\phi)P_T/L$ denote the power assigned to each MT and each column of the AN, where P_T is the total power budget and $\phi \in (0, 1]$ can be used to strike a balance between data transmission and AN emission. Combining (4.12) and (4.10) we obtain

$$y_k^{\mathrm{DL}}(t) = \sqrt{p}\mathbf{g}_k^H(t)\mathbf{f}_k s_k + \sum_{l\neq k}^{K} \sqrt{p}\mathbf{g}_k^H(t)\mathbf{f}_l s_l + \sqrt{q}\mathbf{g}_k^H(t)\mathbf{A}\mathbf{z} + \mathbf{g}_k^H(t)\boldsymbol{\eta}_t^{\mathrm{BS}}(t) + \eta_{r,k}^{\mathrm{MT}}(t) + \xi_k^{\mathrm{DL}}(t), \tag{4.13}$$

where s_k and $\mathbf{f}_k$ denote the k^{th} element of $\mathbf{s}$ and the k^{th} column of matrix $\mathbf{F}$, respectively.

4.2.3 Signal Model of the Eavesdropper

We assume that the eavesdropper is silent during the training phase, i.e., for $t \in \{1, \ldots, B\}$, and eavesdrops the signal intended for MT k during the data transmission phase, i.e., for $t \in \{B+1,\dots,T\}$. Let $\mathbf{G}_E$ denote the channel matrix between the BS and the eavesdropper with i.i.d. zero-mean complex Gaussian elements having variance β_E, where β_E is the path-loss between the BS and the eavesdropper. Since the capabilities of the eavesdropper are not known at the BS, we make worst-case assumptions regarding the hardware and signal processing capabilities of the eavesdropper with respect to communication secrecy. In particular, we assume the received signal at the eavesdropper at time $t \in \{B+1,\dots,T\}$ can be modelled as

$$\mathbf{y}_E(t) = \mathbf{G}_E^H \mathbf{\Psi}^H(t)(\mathbf{x} + \boldsymbol{\eta}_t^{\mathrm{BS}}(t)) \in \mathbb{C}^{N_E \times 1}, \tag{4.14}$$

where $\mathbf{\Psi}(t) = \operatorname{diag}\left(e^{j\psi_1(t)}\mathbf{1}_{1\times N/N_o}^T, \dots, e^{j\psi_{N_o}(t)}\mathbf{1}_{1\times N/N_o}^T\right)$. Thereby, we assumed that the eavesdropper employs high-quality hardware such that the only hardware impairments are the phase noise and the additive distortion noise at the BS. Eq. (4.14) also implies that the thermal noise at the eavesdropper is negligibly small [25, 43, 64]. Furthermore, we assume that the eavesdropper has perfect CSI, i.e., it perfectly knows the effective eavesdropper channel matrix $\mathbf{G}_E^H \mathbf{\Psi}^H(t)$, and can perfectly decode and cancel the interference caused by all MTs except for the MT of interest [25, 43, 64]. These worst-case assumptions lead to an upper bound on the ergodic capacity of the eavesdropper given by

$$C_E = \mathbb{E}[\log_2(1+\gamma_E)] \tag{4.15}$$

where

$$\gamma_E = p\mathbf{g}_E^k \left(\mathbf{G}_E^H(q\mathbf{A}\mathbf{A}^H + \mathbf{\Upsilon}_t^{\mathrm{BS}})\mathbf{G}_E\right)^{-1} (\mathbf{g}_E^k)^H \tag{4.16}$$

and $\mathbf{g}_E^k = \mathbf{f}_k^H \mathbf{G}_E$. We note that since we assumed that the thermal noise at the receiver of the eavesdropper is negligible, γ_E, and consequently C_E, are independent of the path-loss of the eavesdropper, β_E. Furthermore, since perfect channel estimation at the eavesdropper was assumed, the phase noise can be compensated and the only remaining hardware impairment affecting the performance of the eavesdropper is the additive distortion noise at the BS, which impacts the ergodic capacity of the eavesdropper in a similar manner as the AN injected at the BS, cf. (4.16).

4.3 Achievable Ergodic Secrecy Rate in the Presence of Hardware Impairments

In this section, we analyze the achievable ergodic secrecy rate of a massive MIMO system employing non-ideal hardware. To this end, we derive a lower bound on the achievable ergodic secrecy rate in Section 4.3.1, and present an asymptotic analysis for the downlink data rate of the legitimate MTs when MF data precoding is adopted by the BS in Section 4.3.2. In Section 4.3.3, a generalized NS AN precoder is proposed to avoid the AN leakage caused by phase noise for conventional NS AN precoding. Finally, in Section 4.3.4, a simple closed-form upper bound for the eavesdropper's capacity for the new AN precoder is presented.

4.3.1 Lower Bound on Achievable Ergodic Secrecy Rate

In this chapter, we assume that communication delay is tolerable and coding over many independent channel realizations is possible. Hence, we adopt the ergodic secrecy rate achieved by a given MT as performance metric [25].

Before analyzing the secrecy rate, we first employ [22, Lemma 1] to obtain a lower bound on the achievable rate for the multiple-input single-output (MISO) phase noise channel given by (4.10). In particular, the achievable rate of the k^{th} MT, $1 \le k \le K$, in symbol interval $t \in \{B+1,\ldots,T\}$ is lower bounded by

$$R_k(t) \geq \underline{R}_k(t) = \log_2(1+\gamma_k(t)), \tag{4.17}$$

with SINR $\gamma_k(t) =$

$$\frac{p\left|\mathbb{E}\left[\mathbf{g}_k^H(t)\mathbf{f}_k\right]\right|^2}{\sum\limits_{l=1}^{K} p\mathbb{E}\left[\left|\mathbf{g}_k^H(t)\mathbf{f}_l\right|^2\right] - p\left|\mathbb{E}\left[\mathbf{g}_k^H(t)\mathbf{f}_k\right]\right|^2 + \mathbb{E}\left[\mathbf{g}_k^H(t)(q\mathbf{A}\mathbf{A}^H + \mathbf{\Upsilon}_t^{\mathrm{BS}})\mathbf{g}_k(t)\right] + \mathbb{E}\left[\upsilon_{k,r}^{\mathrm{MT}}(t)\right] + \xi^{\mathrm{DL}}}. \tag{4.18}$$

The expectation operator in (4.18) is taken with respect to channel vectors, $\mathbf{g}_k$, as well as the phase noise processes, $\psi_l(t)$ and $\phi_k(t)$. The SINR in (4.18) is obtained by employing the average effective channel gain $\left|\mathbb{E}\left[\mathbf{g}_k^H(t)\mathbf{f}_k\right]\right|$ for signal detection, while treating the deviation from the average effective channel gain as Gaussian noise having variance $\mathbb{E}\left[\left|\mathbf{g}_k^H(t)\mathbf{f}_k\right|^2\right] - \left|\mathbb{E}\left[\mathbf{g}_k^H(t)\mathbf{f}_k\right]\right|^2$, cf. [8]. Moreover, following [22, Lemma 1] we treated the multiuser interference and distortion noises as independent Gaussian noises, which is a worst-case assumption for the calculation of the mutual information. Based on (4.17), we provide a lower bound on the achievable ergodic secrecy rate of the k^{th} MT, $1 \leq k \leq K$, in the following Lemma.

Lemma 4.1. *: The achievable ergodic secrecy rate of the k^{th} MT, $1 \leq k \leq K$, is bounded below by*

$$R_k^{\text{sec}} \geq \underline{R}_k^{\text{sec}} = \frac{1}{T} \sum_{t \in \{B+1,\ldots,T\}} \left[\underline{R}_k(t) - C_E\right]^+, \tag{4.19}$$

where $\underline{R}_k(t)$, $1 \leq k \leq K$, is the lower bound of the achievable ergodic rate of the k^{th} MT given in (4.17) and C_E is the ergodic capacity between the BS and the eavesdropper given in (4.15).

Proof. Please refer to Appendix C.1. □

C_E in (4.19) is constant for all $t \in \{B+1, \ldots, T\}$ as we made the worst-case assumptions that the eavesdropper employs ideal hardware and has perfect CSI. The sum in (4.19) is over the $T-B$ time slots used for data transmission. Motivated by the coding scheme for the non-secrecy case in [77], a similar coding scheme that supports the secrecy rate given in (4.19) is described as follows. For a given $t \in \{B+1, \ldots, T\}$, the statistics of $\mathbf{g}_k(t)$ in (4.18) given the estimate $\hat{\mathbf{g}}_k$ are identical across all coherence intervals and the corresponding channel realizations are i.i.d. Hence, we employ $T-B$ parallel channel codes for each MT; one code for each time $t \in \{B+1, \ldots, T\}$, i.e., the t^{th} channel code is employed across the t^{th} time slots of multiple coherence intervals. Then, at each MT, the t^{th} received symbols across the multiple coherence intervals are jointly decoded [77]. With this coding strategy the ergodic secrecy rate given in (4.19) is achieved provided the parallel codes span sufficiently many (ideally an infinite number) of independent channel realizations $\mathbf{g}_k$ and phase noise samples $\psi_l(t)$ and $\phi_k(t)$.

4.3.2 Asymptotic Analysis of Achievable Rate for MF Precoding

In this subsection, we analyze the lower bound on the achievable ergodic rate of the k^{th} MT, $1 \leq k \leq K$, in (4.17) in the asymptotic limit $N, K \to \infty$ for fixed ratio $\beta = K/N$. Thereby, we adopt MF precoding at the BS, i.e., $\mathbf{f}_k = \hat{\mathbf{g}}_k / \|\hat{\mathbf{g}}_k\|$, as is commonly done for massive MIMO systems because of complexity concerns for more sophisticated precoder designs. In the following Lemma, we provide a closed-form expression for the gain of the desired signal.

Lemma 4.2. *: For MF precoding at the BS, the numerator of (4.18) reflecting the gain of the desired signal at MT $k \in \mathcal{S}_b$, $1 \leq b \leq B_o$, can be expressed as*

$$\mathbb{E}\left[\mathbf{g}_k^H \boldsymbol{\Theta}_k^H(t)\mathbf{f}_k\right] = \sqrt{\beta_k N \lambda_k} \cdot e^{-\frac{\sigma_\psi^2+\sigma_\phi^2}{2}|t-t_0|}, \text{ where } \lambda_k = \beta_k \boldsymbol{\omega}_k^H \boldsymbol{\Theta}_{\sigma(t_0)}^b \boldsymbol{\Sigma}_b^{-1} \boldsymbol{\Theta}_{\sigma(t_0)}^b \boldsymbol{\omega}_k. \tag{4.20}$$

Proof. Please refer to Appendix C.2. □

The term $e^{-\frac{\sigma_\psi^2+\sigma_\phi^2}{2}|t-t_0|}$ in (4.20) reveals the impact of the accumulated phase noise from the time of channel estimation, t_0, to the time of data transmission, t, on the received signal strength at MT k. On the other hand, the phase noise within the training phase affects λ_k, and consequently the received signal strength, via $\boldsymbol{\Theta}_{\sigma(t_0)}^b$ and $\boldsymbol{\Sigma}_b$, cf. (4.5), when multiple pilot sequences are simultaneously emitted in a given training sub-phase. In contrast, when TO pilots are adopted, i.e., only a single user emits pilots in each training sub-phase and $B_b = 1$, $1 \leq b \leq B$, λ_k in (4.20) reduces to $\lambda_k = \frac{p_\tau \beta_k}{p_\tau \beta_k (1+\kappa_t^{\mathrm{MT}}+\kappa_r^{\mathrm{BS}})+\xi^{\mathrm{UL}}}$ and is not affected by the phase noise.

Next, an expression for the multiuser interference power in the first term of the denominator of (4.18) is derived.

Lemma 4.3. *: When MF precoding is adopted at the BS, the power of the multiuser interference caused by the signal intended for the l^{th} MT, $l \neq k$, at MT $k \in \mathcal{S}_b$, $1 \leq b \leq B_o$, is given by*

$$\mathbb{E}\left[\left|\mathbf{g}_k^H \boldsymbol{\Theta}_k^H(t)\mathbf{f}_l\right|^2\right] = \left(\beta_k + \left(X_{k,l}^{(1)} + X_{k,l}^{(2)} + X_{k,l}^{(3)}\right)\left(\frac{1-\epsilon}{N_o} + \epsilon\right)\right), \text{ if } l \in \mathcal{S}_b \tag{4.21}$$

and by β_k otherwise. Here, $\epsilon = e^{-\sigma_\psi^2|t-t_0|}$, $X_{k,l}^{(1)} = \frac{\beta_k^2 \boldsymbol{\omega}_l^H \boldsymbol{\Theta}_{\sigma(t_0)}^b \boldsymbol{\Sigma}_b^{-1} \mathbf{U}_k^b \boldsymbol{\Sigma}_b^{-1} \boldsymbol{\Theta}_{\sigma(t_0)}^b \boldsymbol{\omega}_l}{\boldsymbol{\omega}_l^H \boldsymbol{\Theta}_{\sigma(t_0)}^b \boldsymbol{\Sigma}_b^{-1} \boldsymbol{\Theta}_{\sigma(t_0)}^b \boldsymbol{\omega}_l}$, $X_{k,l}^{(2)} = \frac{N}{N_o} \cdot \frac{\beta_k^2 \boldsymbol{\omega}_l^H \boldsymbol{\Theta}_{\sigma(t_0)}^b \boldsymbol{\Sigma}_b^{-1} \mathbf{W}_k^b \boldsymbol{\Sigma}_b^{-1} \boldsymbol{\Theta}_{\sigma(t_0)}^b \boldsymbol{\omega}_l}{\boldsymbol{\omega}_l^H \boldsymbol{\Theta}_{\sigma(t_0)}^b \boldsymbol{\Sigma}_b^{-1} \boldsymbol{\Theta}_{\sigma(t_0)}^b \boldsymbol{\omega}_l}$, and $X_{k,l}^{(3)} = N\left(1 - \frac{1}{N_o}\right) \cdot \frac{\left|\beta_k \boldsymbol{\omega}_k^H \boldsymbol{\Theta}_{\sigma(t_0)}^b \boldsymbol{\Sigma}_b^{-1} \boldsymbol{\Theta}_{\sigma(t_0)}^b \boldsymbol{\omega}_l\right|^2}{\boldsymbol{\omega}_l^H \boldsymbol{\Theta}_{\sigma(t_0)}^b \boldsymbol{\Sigma}_b^{-1} \boldsymbol{\Theta}_{\sigma(t_0)}^b \boldsymbol{\omega}_l}$.

Proof. Please refer to Appendix C.3. □

Lemma 4.3 confirms that when the number of BS antennas is sufficiently large, i.e., $N \to \infty$, as long as $l \notin \mathcal{S}_b$, the impact of the multiuser interference from the l^{th} MT vanishes, as is commonly assumed in the massive MIMO literature, e.g. [5, 6]. However, the same is not true for MTs that emit pilots in the same training sub-phase as MT k, i.e., MTs $l \in \mathcal{S}_b$. Because of the impairment incurred by the phase noise during the training phase, the interference power of these MTs grows linearly with N and does not vanish compared to the strength of the desired signal in (4.20) in the limit of $N \to \infty$.

Furthermore, for the summand with $l = k$ in the sum in the first term of the denominator of (4.18), we obtain $\mathbb{E}\left[\left|\mathbf{g}_k^H \boldsymbol{\Theta}_k^H(t)\mathbf{f}_k\right|^2\right] =$

$$\mathbb{E}\left[\operatorname{tr}\left(\mathbf{g}_k(t_0)\mathbf{g}_k^H(t_0)\boldsymbol{\Psi}_{t_0}^H(t)\frac{\hat{\mathbf{g}}_k\hat{\mathbf{g}}_k^H}{\|\hat{\mathbf{g}}_k\|^2}\boldsymbol{\Psi}_{t_0}(t)\right)\right] = \beta_k + \beta_k(N-1)\lambda_k\left(\frac{1-\epsilon}{N_o}+\epsilon\right), \quad (4.22)$$

where $k \in \mathcal{S}_b$ and $\boldsymbol{\Psi}_{t_0}(t)$ is defined in Appendix C.2. The last equality in (4.22) is obtained by applying [66, Theorem 1] [61]. The variance of the gain of the desired signal, $\mathbf{g}_k^H \boldsymbol{\Theta}_k^H(t)\mathbf{f}_k$, is obtained by subtracting the right hand side of (4.22) from the square of the right hand side of (4.20).

The two terms in the denominator of (4.18) originating from the hardware impairments at the BS and the k^{th} MT, i.e., $\boldsymbol{\eta}_t^{\text{BS}}(t)$ and $\eta_{r,k}^{\text{MT}}(t)$, respectively, can be calculated as

$$\mathbb{E}\left[\left|\mathbf{g}_k^H \boldsymbol{\Theta}_k^H(t)\boldsymbol{\Upsilon}_t^{\text{BS}}\boldsymbol{\Theta}_k(t)\mathbf{g}_k\right|\right] = \beta_k\kappa_t^{\text{BS}}P_T \quad \text{and} \quad \mathbb{E}\left[\upsilon_{r,k}^{\text{MT}}(t)\right] = \beta_k\kappa_r^{\text{MT}}P_T. \quad (4.23)$$

Substituting the results in (4.20)-(4.23) into (4.18), we obtain the received SINR at

MT $k \in \mathcal{S}_b$ in symbol interval t as

$$\gamma_k(t) = \frac{pN\beta_k\overline{\lambda}_k}{p\beta_k(a_k + c_k) + q\beta_k L_{\mathrm{AN}}^k + \beta_k(\kappa_t^{\mathrm{BS}} + \kappa_r^{\mathrm{MT}})P_T + \xi^{\mathrm{DL}}}, \tag{4.24}$$

with

$$a_k = \sum_{l \in \mathcal{S}_b} \left(1 + \left(X_{k,l}^{(1)} + X_{k,l}^{(2)} + X_{k,l}^{(3)}\right)\left(\frac{1-\epsilon}{N_o} + \epsilon\right)/\beta_k\right) + (K - |\mathcal{S}_b|), \tag{4.25}$$

$$c_k = \left(1 - \frac{1}{N_o}\right)(1-\epsilon) + [(N-1)\lambda_k + 1]\left(\frac{1-\epsilon}{N_o} + \epsilon\right) - N\overline{\lambda}_k, \tag{4.26}$$

where $\overline{\lambda}_k = \lambda_k e^{-(\sigma_\psi^2 + \sigma_\phi^2)|t-t_0|}$. Furthermore, a_k and c_k represent the multiuser interference received at the k^{th} MT and the variance of the gain of the desired signal, respectively. Moreover, the term $L_{\mathrm{AN}}^k = \mathbb{E}\left[\mathbf{g}_k^H \mathbf{\Theta}_k^H(t)\mathbf{A}\mathbf{A}^H\mathbf{\Theta}_k(t)\mathbf{g}_k\right]$ in (4.24) represents the AN leakage in the received signal of the k^{th} MT in time slot t. This term will be characterized in detail for the considered AN precoders in Section 4.3.3.

4.3.3 Generalized NS AN Precoding

The AN leakage term L_{AN}^k in (4.24) depends on the particular AN precoder used. Therefore, in this subsection, we first evaluate L_{AN}^k for the conventional NS precoder, where $\mathbf{A}$ is designed to lie in the NS of the estimated channel vectors of all MTs, $\hat{\mathbf{g}}_k$, $1 \le k \le K$, which is the most common design used in the literature [25, 43, 64]. Subsequently, we propose and analyze the G-NS AN precoder design which is less sensitive to hardware impairments than the conventional NS design.

The AN leakage incurred by the conventional NS AN precoder is given in the following Lemma.

Lemma 4.4. *: For the conventional NS AN precoder, where $L = N - K$ [25, 43, 64],* *the AN leakage power received at MT $k \in \mathcal{S}_b$ in time interval t is given by*

$$L_{\text{AN}}^{k} = \beta_k (N-K)\left(\left(1-\frac{1}{N_o}\right)(1-\epsilon)+1-\lambda_k\right). \tag{4.27}$$

Proof. Please refer to Appendix C.4. □

In Lemma 4.4, the terms ϵ and λ_k reflect the negative impact of the hardware impairments on the AN power leakage. If only one LO is employed, i.e., $N_o = 1$, the impact of ϵ is eliminated. However, the negative effect of ϵ increases as the number of LOs, N_o, increases since the phase noise processes of different LOs are independent destroying the orthogonality of the columns of $\mathbf{A}$ and $\mathbf{g}_k(t)$, $1 \leq k \leq K$.

This problem can be mitigated by employing M_o NS AN precoders where each precoder encodes the data signals intended for the antennas connected to N_o/M_o LOs. Thereby, N_o is assumed to be a multiple of M_o, i.e., $N_o/M_o \in \mathbb{Z}$. The resulting AN preorder is referred to as G-NS AN precoder. More in detail, for the G-NS AN precoder, we divide each channel estimation vector, $\hat{\mathbf{g}}_k$, $1 \leq k \leq K$, into M_o sub-vectors

$$\hat{\mathbf{g}}_k = \left[\left(\hat{\mathbf{g}}_k^{(1)}\right)^T, \left(\hat{\mathbf{g}}_k^{(2)}\right)^T, \dots, \left(\hat{\mathbf{g}}_k^{(M_o)}\right)^T\right]^T, \tag{4.28}$$

where $\hat{\mathbf{g}}_k^{(m)} \in \mathbb{C}^{N/M_o \times 1}$, which contains the $((m-1)N/M_o + 1)^{\text{th}}$ to the $(mN/M_o)^{\text{th}}$ elements of $\hat{\mathbf{g}}_k$ for $1 \leq m \leq M_o$. Correspondingly, we split matrix $\mathbf{A}$ into M_o sub-matrices as follows

$$\mathbf{A} = \left[\mathbf{A}_{(1)}^T, \mathbf{A}_{(2)}^T \dots, \mathbf{A}_{(M_o)}^T\right]^T, \tag{4.29}$$

with $\mathbf{A}_{(m)} \in \mathbb{C}^{N/M_o \times (N/M_o - K)}$, $1 \leq m \leq M_o$, i.e., we have $L = N/M_o - K$. Now, matrix $\mathbf{A}_{(m)}$ is designed to lie in the null-space of $\hat{\mathbf{g}}_k^{(m)}$, $1 \leq k \leq K$, i.e., $\mathbf{A}_{(m)}\hat{\mathbf{g}}_k^{(m)} = \mathbf{0}$, $1 \leq k \leq K$, $1 \leq m \leq M_o$. For $M_o = 1$, the G-NS precoder simplifies to the conventional NS precoder. On the other hand, for $M_o = N_o$, the antennas connected to each LO have their own NS AN precoder.

The AN leakage of the G-NS precoder is analyzed in the following Lemma.

Lemma 4.5. *: For the G-NS AN precoder, where $L = N/M_o - K$ and $1 \leq M_o \leq N_o$, the AN leakage power received at MT $k \in \mathcal{S}_b$ in time interval t is given by*

$$L_{\mathrm{AN}}^{k} = \beta_k \left(\frac{N}{M_o} - K\right)\left(\left(1 - \frac{M_o}{N_o}\right)(1-\epsilon) + 1 - \lambda_k\right). \tag{4.30}$$

Proof. Please refer to Appendix C.5. □

Several observations can be made from (4.30). First, we note that, as expected, for $M_o = 1$, (4.30) reduces to (4.27). Second, the negative impact of the phase noise via ϵ on the AN leakage can be completely eliminated by choosing $M_o = N_o$. Third, the G-NS precoder requires the calculation of M_o null spaces of dimension $N/M_o \times K$. Hence, computational complexity increases with M_o. We will elaborate on the optimal choice of M_o in Sections 4.4 and 4.5.

The achievable rates of MT $k \in \mathcal{S}_b$ in time slot t with conventional NS and G-NS precoding are obtained by inserting (4.27) and (4.30) into (4.24), respectively. Hence, for the proposed G-NS precoder, we obtain

$$\underline{R}_k(t) = \log_2\left(1 + \frac{\overline{\lambda}_k \phi N}{(a_k + c_k - \beta\mu_k)\phi + \beta\mu_k + \xi_k}\right), \tag{4.31}$$

where $\mu_k = (\frac{N}{M_o} - K)\left(\left(1 - \frac{M_o}{N_o}\right)(1-\epsilon) + 1 - \lambda_k\right)$, $\xi_k = \beta(\kappa_r^{\mathrm{MT}} + \kappa_t^{\mathrm{BS}} + \xi^{\mathrm{DL}}/(\beta_k P_T))$, and $\beta = K/N > 0$.

4.3.4 Upper Bound on the Eavesdropper's Capacity

In the following Proposition, we provide a tight and tractable upper bound on eavesdropper's capacity.

Proposition 4.1. *: For $N \to \infty$ and (G-)NS AN precoding, the eavesdropper's capacity in (4.15) can be upper bounded as*

$$C_E \leq \overline{C}_E = \log_2\left(1 + \frac{pN_E}{qL + \kappa_t^{\mathrm{BS}} P_T - \chi N_E}\right), \text{ with } \chi = \frac{(1+\kappa_t^{\mathrm{BS}})^2 q^2 L + (\kappa_t^{\mathrm{BS}})^2 p^2 K}{(1+\kappa_t^{\mathrm{BS}}) qL + \kappa_t^{\mathrm{BS}} pK}, \tag{4.32}$$

for $qL + \kappa_t^{\mathrm{BS}} P_T > \chi N_E$, and where $L = N - K$ and $L = N/M_o - K$ for the conventional NS and the G-NS precoders, respectively.

Proof. The term $\mathbf{G}_E^H \mathbf{\Upsilon}_t^{\mathrm{BS}} \mathbf{G}_E$ in (4.16) converges to a deterministic diagonal matrix for $N \to \infty$, and is therefore independent of $\mathbf{g}_E^k$. Hence, similar steps as in [43, Appendix B, C] can be used to arrive at (4.32). □

We observe from (4.32) that, as expected, the capacity of the eavesdropper is increasing in the number of its equipped antennas, N_E. Interestingly, when no AN is injected, i.e., $q = 0$, (4.32) reduces to

$$\overline{C}_E \bigg|_{q=0} = \log_2\left(1 + \frac{N_E}{\kappa_t^{\mathrm{BS}}(K - N_E)}\right), \tag{4.33}$$

for $K > N_E$. For perfect BS hardware, we have $\kappa_t^{\mathrm{BS}} \to 0$ and $\overline{C}_E \to \infty$ making secure communication impossible. Hence, without AN injection, hardware impairments may in fact be beneficial for secure communication as the distortion noise at the BS acts like AN and may facilitate secrecy. This surprising insight will be studied more carefully in the next section. Furthermore, the number of independent distortion noise processes at the BS is equal to the number of users, K. Hence, $K > N_E$ is needed to prevent the eavesdropper from nulling out the distortion noise and for achieving secrecy.

4.4 Guidelines for System Design

In this section, we exploit the analytical results derived in the previous section to gain some insight into the impact of the various system and hardware impairment parameters on system design. To this end, we carefully study the closed-form lower bound on the achievable ergodic secrecy rate obtained by combining (4.19), (4.31), and (4.32).

4.4.1 Design of the Pilot Sequences

Assuming that we assign the maximum number of users to each training sub-phase, i.e., $|\mathcal{S}_b| = B_b$, the relevant design parameter for the pilot sequences is the number of training sub-phases B_o, or equivalently, the size of the training sub-phases B_b as $\sum_{b=1}^{B_o} B_b = B$. In particular, B_b affects the lower bound on the achievable ergodic rate of MT k in (4.31) via λ_k, a_k, and c_k, where c_k becomes proportional to λ_k for $N \to \infty$, cf. (4.26). Thereby, close inspection of (4.20) reveals that λ_k, which reflects the power of the received useful signal, is not monotonic in B_b. This can be explained as follows. On the one hand, since the power of each pilot symbol is constrained, i.e., $|\omega_k(t)|^2 = p_\tau$, $\forall k, t$, the sum power of the pilot sequence per MT increases with B_b. On the other hand, for larger B_b, more MTs are allowed to emit pilots in training sub-phase b introducing more contamination due to phase noise. This has an adverse effect on the quality of the channel estimate and consequently on the power of the received useful signal. Similarly, close inspection of (4.25) reveals that a_k, which reflects the multiuser interference incurred to the k^{th} MT, is a monotonically increasing function of B_b, as a lower channel estimation accuracy gives rise to more multiuser interference. Considering the behaviour of λ_k, a_k, and c_k and their impact on the achievable ergodic rate of MT k in (4.31), we conclude that B_b, $1 \leq b \leq B_o$, should be optimized and the optimal value depends on the channel and hardware impairment parameters. Thereby, the optimal B_b is decreasing in the phase noise variances, σ^2_ψ and σ^2_ϕ, as the degradation introduced by concurrent pilot emission by multiple MTs is increasing in these parameters. This conclusion will be verified in Section 4.5.2 by numerically evaluating (4.19).

4.4.2 Selection of M_o for G-NS AN Precoding

The number of G-NS AN precoding sub-matrices, M_o, $1 \leq M_o \leq N_o$, employed affects the achievable ergodic secrecy rate via the AN leakage L^k_{AN} in (4.30) and via the (bound on the) eavesdropper capacity $\overline{C}_E$ in (4.32). The AN leakage is a decreasing function with respect to M_o, i.e., as far as the AN leakage is concerned, $M_o = N_o$ is preferable. On the other hand, since the dimensionality of the G-NS AN precoder is given by $L = N/M_o - K$, the eavesdropper capacity is an increasing function of M_o, cf. (4.32), which has a negative effect on the ergodic secrecy rate. Hence, M_o has to be optimized. Since the eavesdropper capacity does not depend on the phase noise, we expect that the optimal M_o increases with increasing BS phase noise variance, σ^2_ψ, as σ^2_ψ affects the AN leakage via ϵ in (4.30). This conjecture will be numerically verified in Section 4.5.4.

4.4.3 Secrecy in the Absence of AN

In [43, 64] it was shown that if perfect hardware is employed, injection of AN is necessary to achieve secrecy. In particular, without AN generation, under worst-case assumptions regarding the noise at the eavesdropper, the eavesdropper capacity is unbounded. On the other hand, we showed in Section 4.3.4 that in the presence of hardware impairments the eavesdropper capacity is bounded since the distortion noise generated at the BS has a similar effect as AN. Motivated by this observation, in this section, we calculate the maximum number of eavesdropper antennas N_E that can be tolerated if a positive secrecy rate is desired without AN emission.

If AN is not emitted, we have $\phi = 1$ or $q = 0$. In this case, the proposed lower bound on the ergodic secrecy rate of the k^{th} MT in time interval t simplifies to

$$\underline{R}_k^{\text{sec}}(t)\bigg|_{q=0} = \left[\log_2\left(1 + \frac{\overline{\lambda}_k N}{a_k + c_k + \xi_k}\right) - \log_2\left(1 + \frac{\alpha}{\kappa_t^{\text{BS}}(\beta - \alpha)}\right)\right]^+. \tag{4.34}$$

where $\alpha = N_E/N$ denotes the normalized number of eavesdropper antennas. In the following Proposition, we provide a condition for the number of eavesdropper antennas that has to be met for secure communication to be possible.

Proposition 4.2. *: If AN is not generated, the maximum number of eavesdropper antennas that the system can tolerate while ensuring a positive ergodic secrecy rate is* $N_E = \lfloor \alpha_{\text{AN}} N \rfloor$, *where*

$$\alpha_{\text{AN}} = \frac{\overline{\lambda}_k N \kappa_t^{\text{BS}} \beta}{\overline{\lambda}_k N \kappa_t^{\text{BS}} + a_k + c_k + \xi_k}\bigg|_{t=B+1}. \tag{4.35}$$

Proof. First, we note that $\underline{R}_k(t)$ is a decreasing function of t. Hence, considering (4.19), it is sufficient to ensure $\underline{R}_k(B+1) > \overline{C}_E$ for achieving a positive ergodic secrecy rate. Eq. (4.35) is obtained by setting (4.34) to zero and observing that $\underline{R}_k^{\text{sec}}(t)\Big|_{q=0}$ is a decreasing function of α. □

Eq. (4.35) clearly shows that the additive distortion noise at the BS is essential for achieving a positive secrecy rate if AN is not injected as $\alpha_{\text{AN}} = 0$ results if $\kappa_t^{\text{BS}} = 0$.

On the other hand, α_{AN} is a decreasing function of all other hardware impairment parameters, i.e., κ_r^{BS}, κ_t^{MT}, κ_r^{MT}, ξ^{DL}, σ_ψ^2, and σ_ψ^2, as the corresponding hardware impairments affect only the achievable ergodic rate of the MT but not the ergodic capacity of the eavesdropper. We note that α_{AN} is an increasing function of β since the dimensionality of the additive distortion noise at the BS is proportional to β.

4.4.4 Maximum Number of Eavesdropper Antennas

Now, we consider the maximum number of eavesdropper antennas that can be tolerated if a positive ergodic secrecy rate is desired and AN injection is possible. Combining (4.19), (4.31), and (4.32), the lower bound on the ergodic secrecy rate in time interval t can be expressed as

$$\underline{R}_k^{\mathrm{sec}}(t) = \left[\log_2\left(1+\frac{\overline{\lambda}_k\phi N}{(a_k+c_k)\phi+\beta\mu_k(1-\phi)+\xi_k}\right)-\log_2\left(1+\frac{\alpha\phi}{\beta(1-\phi+\kappa_t^{\mathrm{BS}}-\chi'\alpha)}\right)\right]^+, \tag{4.36}$$

where $\chi' = \frac{(1+\kappa_t^{\mathrm{BS}})^2(1-\phi)^2N/L+(\kappa_t^{\mathrm{BS}})^2\phi^2/\beta}{1-\phi+\kappa_t^{\mathrm{BS}}}$.

Proposition 4.3. : *If AN injection is possible, a positive secrecy rate can be achieved by the k^{th} MT if the number of eavesdropper antennas does not exceed $N_E = \lfloor \alpha_{\mathrm{sec}} N \rfloor$, where*

$$\alpha_{\mathrm{sec}} = \frac{(1+\kappa_t^{\mathrm{BS}})\overline{\lambda}_k L}{L/N(\mu_k+\kappa_r^{\mathrm{MT}}+\kappa_t^{\mathrm{BS}}+\xi^{\mathrm{DL}}/(\beta_k P_T))+\overline{\lambda}_k N(1+\kappa_t^{\mathrm{BS}})}\Big|_{t=B+1} \tag{4.37}$$

and $\phi \to 0$, i.e., almost all transmit power is employed for AN generation.

Proof. Exploiting again that $\underline{R}_k(t)$ is a decreasing function of t it suffices to consider the ergodic secrecy rate for $t = B+1$. Then, an expression for α_{sec} is obtained by setting $\underline{R}_k^{\mathrm{sec}}(t)$ in (4.36) to zero. This expression is monotonically decreasing in ϕ and hence can be further simplified by letting $\phi \to 0$ which yields (4.37). □

Proposition 4.3 reveals that, as expected, the number of eavesdropper antennas that can be tolerated increases with the channel estimation accuracy (i.e., $\overline{\lambda}_k$) and the number of spatial dimensions available for AN (i.e., L). Furthermore, similar to α_{AN}, α_{sec} is a decreasing function of the hardware impairment parameters κ_r^{BS}, κ_t^{MT}, κ_r^{MT}, ξ^{DL}, σ_ψ^2, and σ_ψ^2, and an increasing function of κ_t^{BS}. However, unlike α_{AN}, α_{sec} is independent of β.

4.4.5 Number of LOs

The number of LOs, N_o, affects the ergodic secrecy rate via the terms a_k, c_k, and μ_k in the achievable ergodic rate in (4.31). For $N \to \infty$, a_k and c_k are decreasing functions of N_o, i.e., less multiple access interference is caused if more LOs are employed, whereas the AN leakage term μ_k is an increasing function in N_o. Therefore, considering the specific form of the denominator of the fraction inside the logarithm in (4.31), the optimal value of N_o, which maximizes the ergodic secrecy rate, depends on ϕ. In particular, for a given M_o, for $\phi = 1$ no AN is injected and μ_k cancels in the expression for the achievable ergodic rate in (4.31). Hence, in this case, the ergodic secrecy rate is a monotonically increasing function of N_o, i.e., increasing the number of LOs is beneficial. On the other hand, for a given M_o, for $\phi < 1$, the optimal N_o maximizing the ergodic secrecy rate can be found by performing a numerical search based on (4.31).

We note that by employing G-NS AN generation and enforcing $M_o = N_o$, we can avoid the harmful effect of the multiple LOs on the AN leakage term μ_k. In this case, the achievable ergodic rate of the MT becomes an increasing function of $M_o = N_o$. However, at the same time, the number of dimensions available for AN injection, $L = N/M_o - K$, is a decreasing function of $M_o = N_o$. Therefore, the optimal $M_o = N_o$ maximizing the ergodic secrecy rate has to be found again by a numerical search.

4.4.6 Are hardware impairments Beneficial for Security?

Since the hardware impairment parameters κ_r^{BS}, κ_t^{MT}, κ_r^{MT}, ξ^{DL}, σ_ψ^2, and σ_ψ^2 only affect the legitimate user but not the eavesdropper, the corresponding hardware impairments are always detrimental to the ergodic secrecy rate. However, the additive distortion noise at the BS affects both the achievable ergodic rate of the MT and the capacity of the eavesdropper. Hence, it is not a priori clear if this hardware impairment is beneficial or detrimental to the ergodic secrecy rate. The following Proposition provides a criterion for judging the benefits of the additive BS distortion noise.

Proposition 4.4. *: For time interval t, non-zero additive BS distortion noise with small $\kappa_t^{\mathrm{BS}} > 0$, $\kappa_t^{\mathrm{BS}} \to 0$, is beneficial for the achievable ergodic secrecy rate of the k^{th} MT if and only if*

$$(1-\phi)[1 - N_E/L - (1 - N_E/L - N_E/K)\phi] \times \frac{1 - N_E/L}{1 - (1-2\phi)N_E/L} < \frac{\alpha\gamma(N\overline{\lambda}_k\phi + \gamma)}{\beta^2\overline{\lambda}_k N}, \tag{4.38}$$

where $\gamma = (a_k + c_k)\phi + \beta\mu_k(1-\phi) + \beta(\kappa_r^{\mathrm{MT}} + \xi^{\mathrm{DL}}/(\beta_k P_T))$.

Proof. For additive BS distortion noise to be beneficial for a given time interval t and small $\kappa_t^{\mathrm{BS}} > 0$, the derivative $\partial \underline{R}_k^{\mathrm{sec}}(t)/\partial\kappa_t^{\mathrm{BS}}$ at $\kappa_t^{\mathrm{BS}} = 0$ has to be positive. Assuming $\underline{R}_k^{\mathrm{sec}}(t) > 0$, this condition leads to $\partial \underline{R}_k(t)/\partial\kappa_t^{\mathrm{BS}}|_{\kappa_t^{\mathrm{BS}}=0} > \partial\overline{C}_E/\partial\kappa_t^{\mathrm{BS}}|_{\kappa_t^{\mathrm{BS}}=0}$, which can be further simplified to (4.38). □

Remark 4.1. *: We note that the criterion in Proposition 4.4 only guarantees that additive BS distortion noise with small positive κ_t^{BS} is beneficial. The ergodic secrecy rate, $\underline{R}_k^{\mathrm{sec}}(t)$, is in general not monotonic in κ_t^{BS} and larger κ_t^{BS} may be harmful even if small κ_t^{BS} are beneficial, see Section 4.5.5. Furthermore, since the right hand side of (4.38) is always positive, we conclude that additive BS distortion noise with small κ_t^{BS} is always beneficial when $\phi = 1$, i.e., when AN is not injected.*

4.5 Numerical Examples

In this section, we provide numerical and simulation results to verify the analysis presented in Sections 4.3 and 4.4 and to illustrate the impact of hardware impairments on the ergodic secrecy rate. For the numerical results, we numerically evaluate the analytical expression for the lower bound on the ergodic secrecy rate obtained by combining (4.19), (4.31), and (4.32). For the simulation results, we employ Monte Carlo simulation and evaluate (4.19) using $\underline{R}_k^{\mathrm{sec}}(t) = \log_2(1+\gamma_k(t))$ and $C_E = \log_2(1+\gamma_E)$ with $\gamma_k(t)$ and γ_E given by (4.18) and (4.16), respectively, for $5,000$ independent channel realizations. For simplicity, in this section, we assume that the path-loss for all MTs is identical, i.e., $\beta_k = 1$, $1 \leq k \leq K$, and the coherence block length is equal to $T = 500$ time slots. Typical values for the phase noise increment standard deviations, σ_ψ, σ_ϕ, used include $0.06°$, which was adopted in the long-term evolution (LTE) specifications [78], and $6°$, which corresponds to strong phase noise according to [79, 80]. Furthermore, typical values for the additive distortion noise $\kappa_t^{\mathrm{MT}} = \kappa_r^{\mathrm{BS}} = \kappa_t^{\mathrm{BS}} = \kappa_r^{\mathrm{MT}}$ include $\{0, 0.05^2, 0.15^2\}$ [18], whereas the amplified receiver noise was set to $\xi^{\mathrm{UL}} = \xi^{\mathrm{DL}} = 1.58\sigma_n^2$ [22], with $\sigma_n^2 = 1$. The specific values of the adopted system and hardware impairment parameters are provided in the captions of the figures.

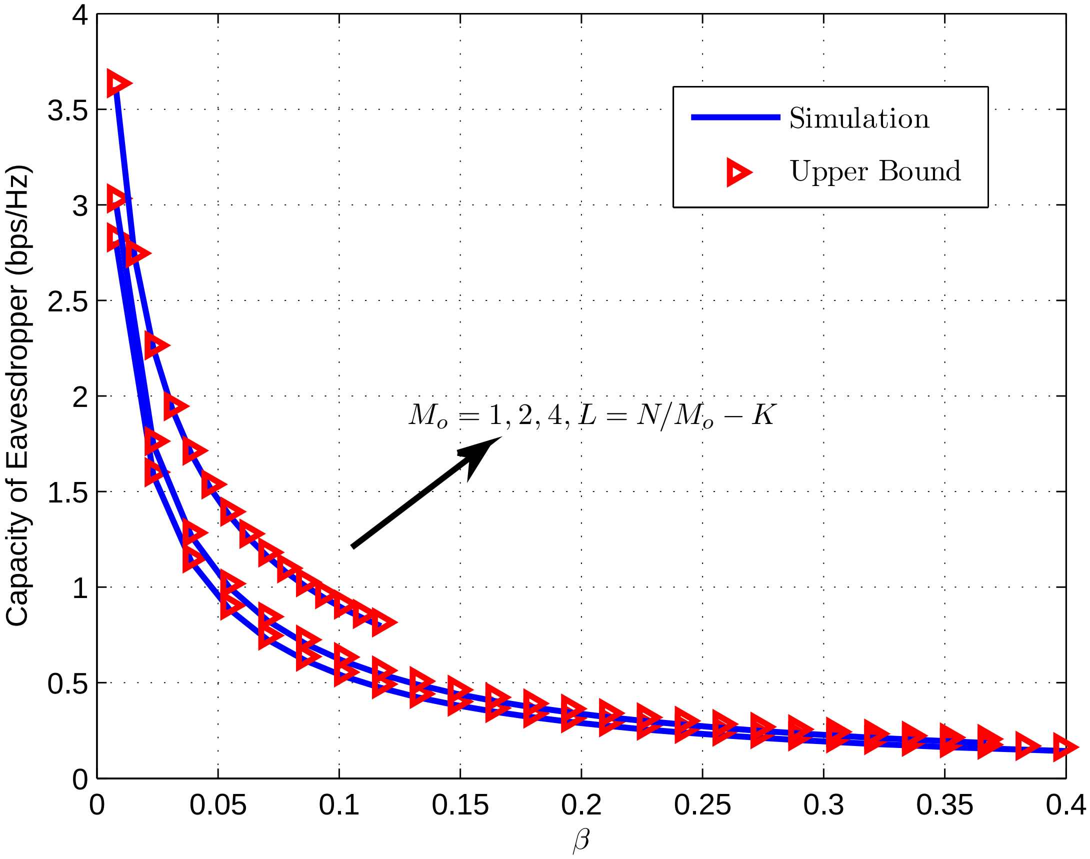

Figure 4.2: Capacity of the eavesdropper vs. the normalized number of MTs β for a system with $N = 128$, $N_o = 4$, $N_E = 16$, $P_T = 10$ dB, $\phi = 0.25$, $\kappa_t^{\text{BS}} = 0.15^2$, and G-NS AN precoding with $M_o = \{1, 2, 4\}$.

4.5.1 Capacity of Eavesdropper for G-NS AN Precoding

Fig. 4.2 depicts the eavesdropper's ergodic capacity, C_E, as a function of β for G-NS AN precoding with $M_o = \{1, 2, 4\}$. Besides results for the analytical upper bound, $\overline{C}_E$, from (4.32), we also show simulation results for C_E by averaging $\log_2(1+\gamma_E)$ over $5,000$ independent channel realizations, where γ_E is given by (4.16). From Fig. 4.2 we observe that the proposed upper bound on the capacity of the eavesdropper is very tight. Furthermore, as expected, the ergodic capacity of the eavesdropper is an increasing function of M_o since the number of dimensions available for AN generation, $L = N/M_o - K$, is a decreasing function of M_o. In fact, since $L = N/M_o - K > N_E$ is needed for successfully jamming the eavesdropper, for $M_o = 4$, we depict the ergodic capacity of the eavesdropper only for $\beta < 0.125$. Nevertheless, as will be shown below, choosing $M_o > 1$ may still be beneficial as far as the ergodic secrecy rate is concerned as the achievable ergodic rate of the MT is an increasing function of M_o.

4.5.2 Achievable Ergodic Rate of MT for Different Pilot Designs

Next, we investigate the impact of the general pilot designs introduced in Section 4.2.1 on the lower bound of the achievable ergodic rate of the considered MT given in (4.31)[7]. Note that the capacity of the eavesdropper is not affected by the pilot design. For simplicity, we assume equal duration for all training sub-phases, $B_b = B/B_o$, $b \in \{1, \dots, B_o\}$, and $B = K$. The same number of users is assigned to each training sub-phase. In Fig. 4.3, we show the achievable ergodic rate of a MT in training set $\mathcal{S}_{B_o}$ as well as the corresponding $\overline{\lambda}_k$, which reflects the power of the received useful signal, and a_k, which reflects the multiuser interference. Results for $B_o = 1$ (SO pilots), $B_o = 2$, and $B_o = 16$ (TO pilots) are shown. As predicted in Section 4.4.1, the multiuser interference, a_k, is monotonically decreasing in B_o as larger B_o improve the robustness against phase noise during the channel estimation phase, which allows better suppression of multiuser interference via MF precoding. Somewhat surprisingly, for $\sigma_\psi = \sigma_\phi \leq 5^\circ$, a_k is a decreasing function of the phase noise variance. This may be attributed to the fact that phase noise prevents the coherent

[7] We note that all results obtained by numerically evaluating the analytical expressions derived in this chapter were verified by simulations. However, the simulation results are not included in all figures for clarity of presentation.

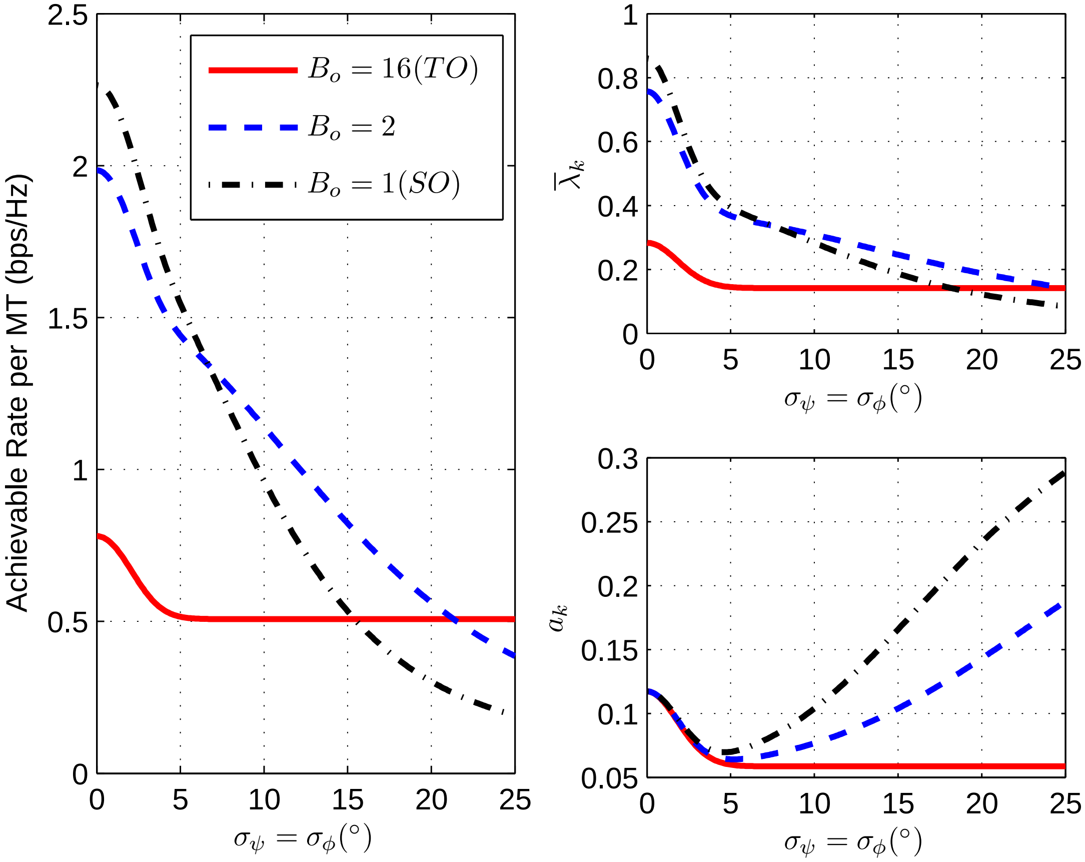

Figure 4.3: Achievable ergodic rate, $\overline{\lambda}_k$, and a_k vs. phase noise standard deviation $\sigma_\psi = \sigma_\phi$ for different pilot designs for a system with $N = 128$, $N_o = 2$, $N_E = 16$, $K = 16$, $p_\tau = P_T/K$, $P_T = 10$ dB, $\phi = 0.5$, and $\kappa_t^{\mathrm{BS}} = \kappa_r^{\mathrm{BS}} = \kappa_t^{\mathrm{MT}} = \kappa_r^{\mathrm{MT}} = 0.05^2$.

superposition of the multiuser interference generated by different MTs such that large interference values are avoided. On the other hand, for $\sigma_\psi = \sigma_\phi > 5^\circ$, the detrimental effects of the pilot contamination caused by the loss of orthogonality for $B_o < 16$ outweigh this positive effect and a_k increases with the phase noise variance. For $\overline{\lambda}_k$, i.e., the received signal power, we observe from Fig. 4.3 that the optimal B_o depends on the phase noise variance. In particular, for small phase noise variances, small B_o are preferable since the increased pilot power outweighs the loss of orthogonality during training. On the other hand, for large phase noise variances, eventually TO pilots become optimal as the preserved orthogonality during training becomes crucial. The behaviour of $\overline{\lambda}_k$ and a_k is also reflected in the behaviour of the achievable rate of the considered MT. In particular, for the considered system parameters, $B_o = 1$, $B_o = 2$, and $B_o = 16$ are optimal for $\sigma_\psi = \sigma_\phi \leq 6^\circ$, $6^\circ < \sigma_\psi = \sigma_\phi \leq 21^\circ$, and $\sigma_\psi = \sigma_\phi > 21^\circ$ (which is not a practical range), respectively. Hence, in practice, the optimal B_o can be found by evaluating (4.31).

4.5.3 Optimal Power Allocation to Data and AN

Fig. 4.4 shows the achievable ergodic secrecy rate as a function of the power allocation parameter ϕ for SO and TO pilots and different phase noise variances. G-NS AN precoding with $M_o = N_o = 2$ is adopted. The curve for ideal hardware components, i.e., $\kappa_t^{\mathrm{BS}} = \kappa_r^{\mathrm{BS}} = \kappa_t^{\mathrm{MT}} = \kappa_r^{\mathrm{MT}} = \sigma_\psi = \sigma_\phi = 0$, is also provided for reference. We investigate the optimal power allocation between data transmission and AN emission for the maximization of the ergodic secrecy rate achieved for different phase noise levels. When the phase noise variance is small, i.e., $\sigma_\psi = \sigma_\phi = 0.6^\circ$, SO pilots outperforms TO pilots for all values of ϕ. However, this is not true for stronger phase noise. We also observe that the optimal value for ϕ maximizing the ergodic secrecy rate is only weakly dependent on the phase noise variance.

4.5.4 Achievable Ergodic Secrecy Rate for Non-Ideal Hardware Components

In Fig. 4.5, we show the ergodic secrecy rate achieved with G-NS AN precoding for different values of M_o as a function of the number of BS antennas. The cases of weak ($\sigma_\psi = \sigma_\phi = 0.6^\circ$) and strong ($\sigma_\psi = \sigma_\phi = 6^\circ$) phase noise are considered. For weak phase noise, using large values of M_o becomes beneficial only for large numbers of

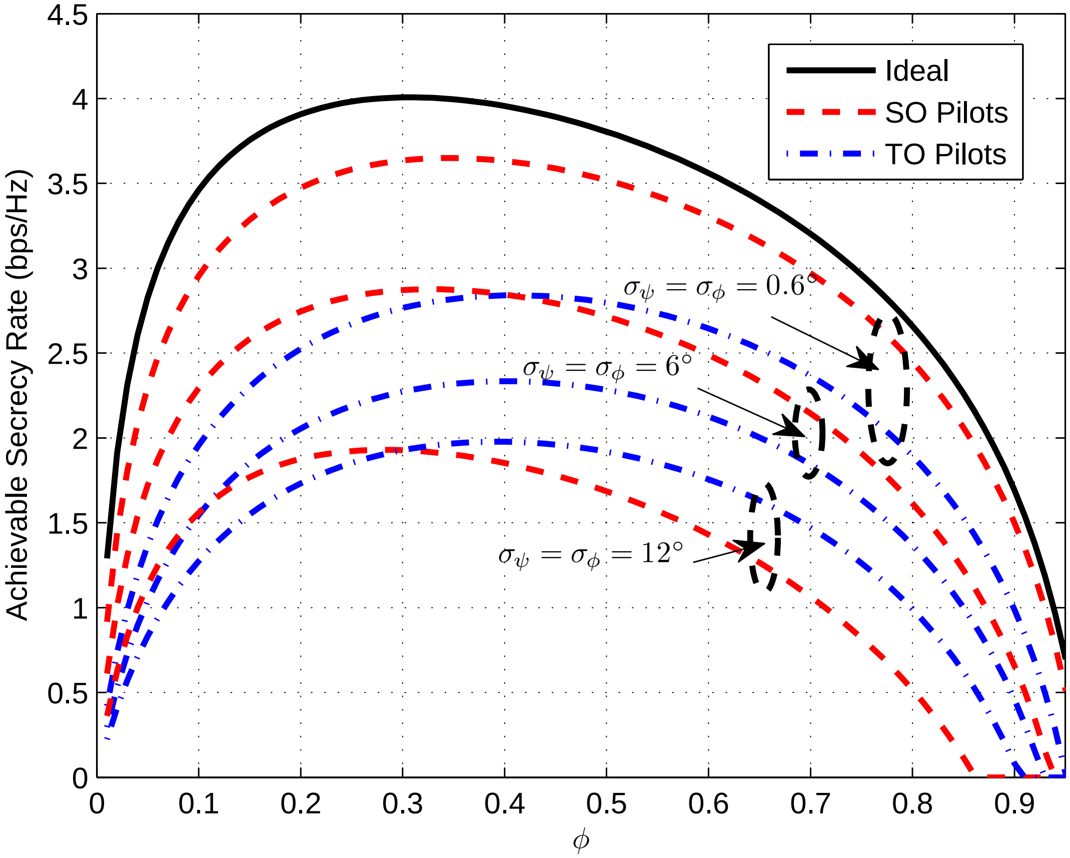

Figure 4.4: Achievable ergodic secrecy rate vs. ϕ for SO and TO pilots and a system with $K = 4$, $N = 128$, $N_o = M_o = 2$, $N_E = 4$, $p_\tau = P_T/K$, $P_T = 10$ dB, and $\kappa_t^{\text{BS}} = \kappa_r^{\text{BS}} = \kappa_t^{\text{MT}} = \kappa_r^{\text{MT}} = 0.15^2$.

antennas, i.e., $N > 200$, as for smaller numbers of antennas the positive effect of larger values of M_o on the AN leakage is outweighed by their negative effect on the number of spatial dimensions available for AN precoding. On the other hand, for strong phase noise, the AN leakage is larger and its mitigation by choosing $M_o = N_o = 16$ is beneficial already for $N > 150$. These observations are in line with our theoretical considerations in Section 4.4.2. Fig. 4.5 also confirms the accuracy of the derived analytical expressions for the ergodic secrecy rate.

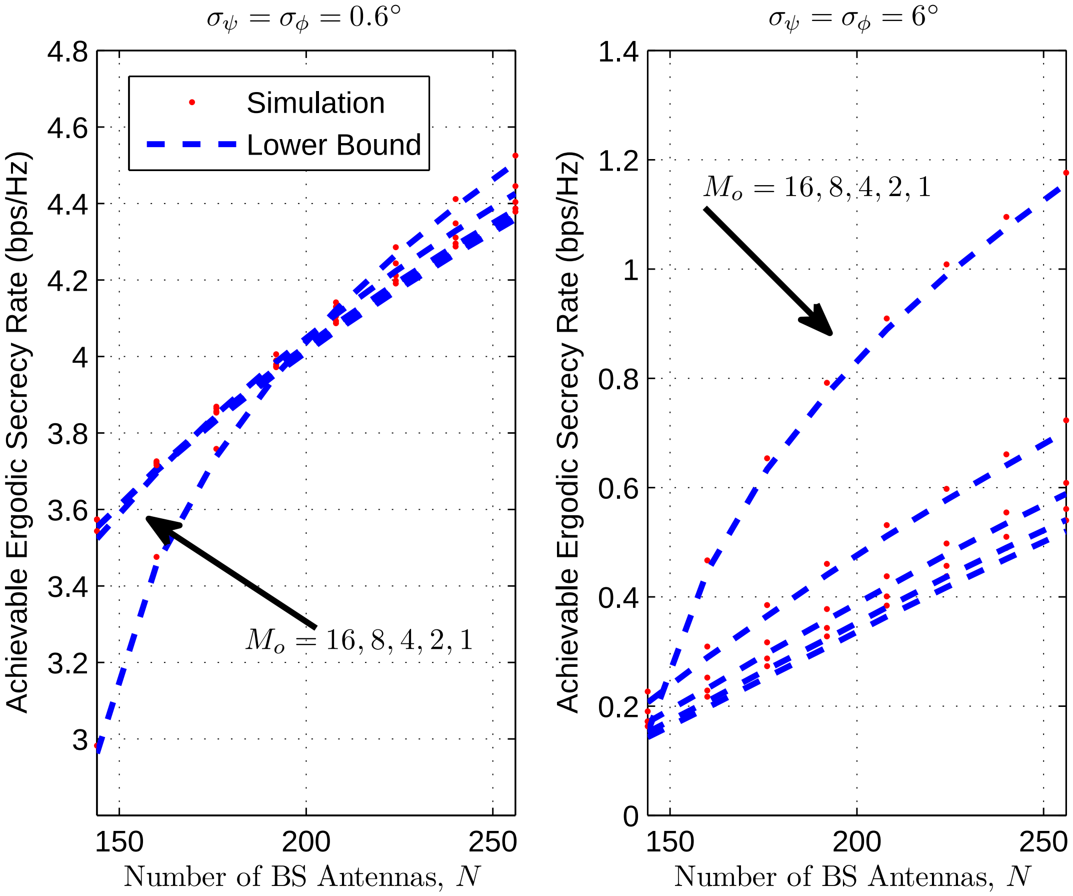

Figure 4.5: Achievable ergodic secrecy rate vs. number of BS antennas for G-NS AN precoding and a system with $K = 4$, $N_E = 4$, $N_o = 16$, $B_o = 1$, $p_\tau = P_T/K$, $P_T = 10$ dB, and $\kappa_t^{\text{BS}} = \kappa_r^{\text{BS}} = \kappa_t^{\text{MT}} = \kappa_r^{\text{MT}} = 0.15^2$. The optimal ϕ is adopted.

4.5.5 Maximum Tolerable Number of Eavesdropper Antennas

Fig. 4.6 depicts the (normalized) maximum tolerable number of eavesdropper antennas for achieving a positive ergodic secrecy rate for the case without AN generation, α_{AN}, and the case with AN generation, α_{sec}, as a function of the (normalized) number of users, β. Results for channel estimation based on SO and TO pilots as well as the case of no phase noise ($\sigma_\psi = \sigma_\phi = 0°$) are shown for $N_o = 2$ and $N_o = 4$

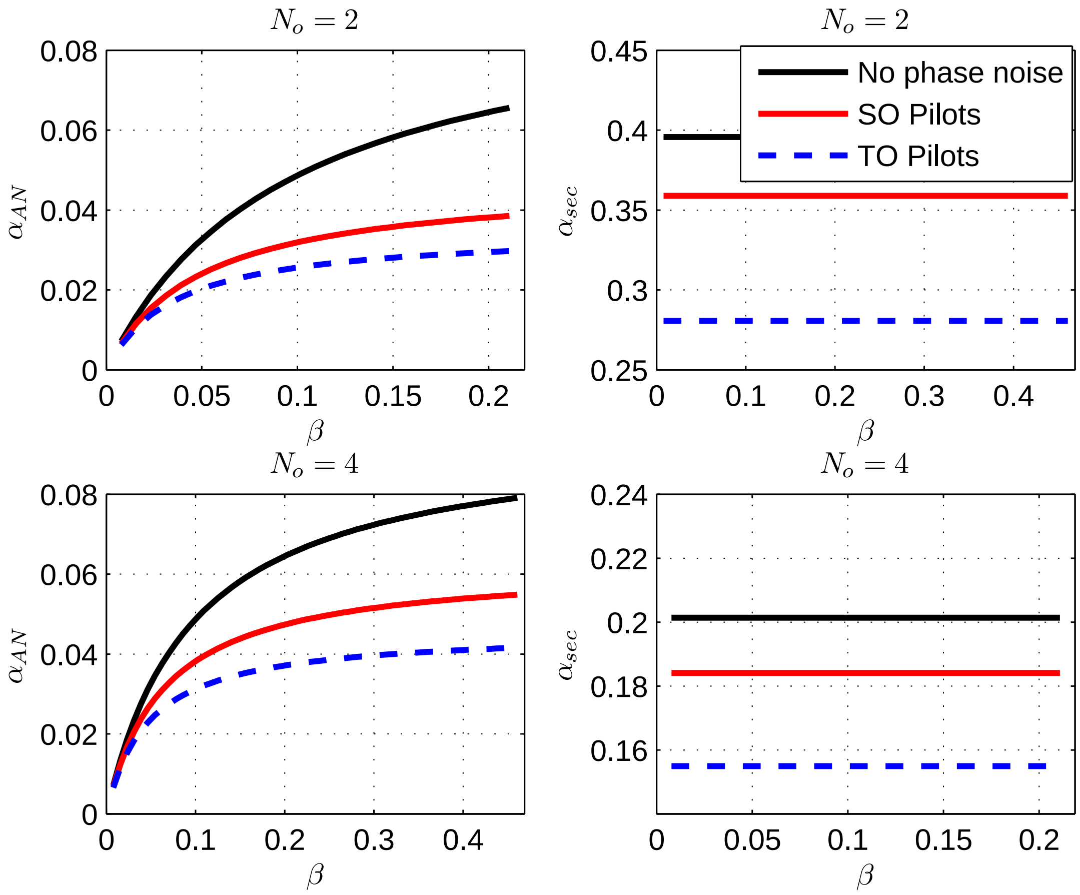

Figure 4.6: α_{AN} and α_{sec} vs. the normalized number of MTs β for SO and TO pilots and a system with $N = 128$, $M_o = 2$, $p_\tau = P_T/K$, $P_T = 10$ dB, $\sigma_\psi = \sigma_\phi = 6°$, and $\kappa_t^{\text{BS}} = \kappa_r^{\text{BS}} = \kappa_t^{\text{MT}} = \kappa_r^{\text{MT}} = 0.15^2$.

LOs. First, we note that, as expected from our considerations in Section 4.4.5, for the case without AN ($\phi = 1$), increasing N_o from 2 to 4 is beneficial, i.e., the number of tolerable eavesdropper antennas increases. In contrast, if AN is injected, $N_o = 2$ is preferable. Second, AN generation is beneficial and improves the robustness against eavesdropping, i.e., $\alpha_{\text{sec}} > \alpha_{\text{AN}}$. Third, as expected from Sections 4.4.3 and 4.4.4, α_{AN} is a monotonically increasing function of β whereas α_{sec} is independent of β. Fourth, for the considered example of weak phase noise, SO pilots outperform the TO pilots for all considered cases.

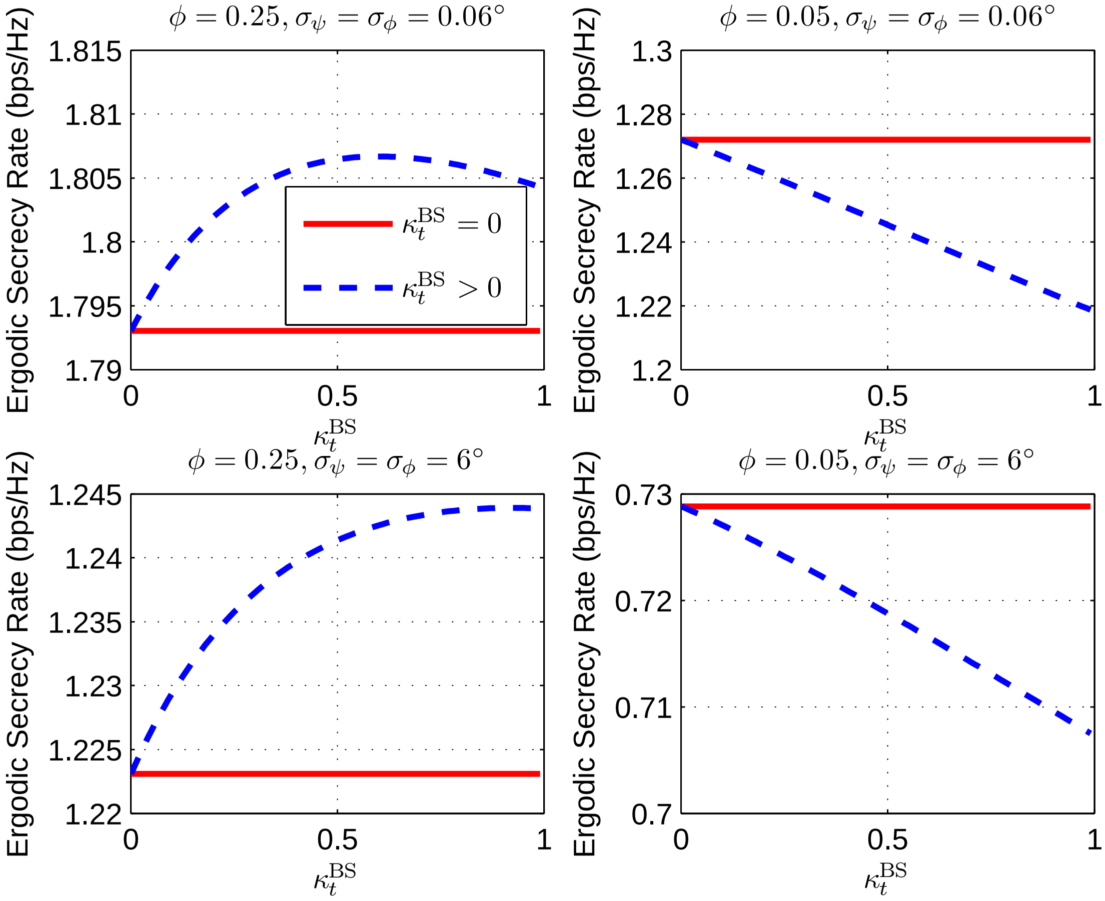

Figure 4.7: Achievable ergodic secrecy rate vs. BS distortion noise parameter κ_t^{BS} for a system with $N = 128$, $K = 32$, $N_E = 4$, $N_o = M_o = 2$, $p_\tau = P_T/K$, $P_T = 10$ dB, and $\kappa_r^{\mathrm{BS}} = \kappa_t^{\mathrm{MT}} = \kappa_r^{\mathrm{MT}} = 0.15^2$.

4.5.6 Is Additive Distortion Noise at the BS Beneficial for Security?

In Fig. 4.7, we show the achievable ergodic secrecy rate as a function of the BS distortion noise parameter, κ_t^{BS}, for different phase noise variances and different power allocation factors ϕ. For comparison, the achievable ergodic secrecy rates without BS distortion noise (i.e., $\kappa_t^{\mathrm{BS}} = 0$) are also shown. Fig. 4.7 shows that if the power allocated to AN is substantial (e.g., $\phi = 0.05$), the additional distortion noise has a negative effect on the ergodic secrecy rate. On the other hand, if the power assigned for AN is not sufficient (e.g., $\phi = 0.25$), non-zero additive distortion noise at the BS is beneficial as the distortion noise acts like additional AN. In particular, for $\phi = 0.25$, $\sigma_\psi = 0.06°$, we obtain for the left hand side and right hand side of (4.38) 0.52 and 1.66, respectively, which we represent as $(0.52, 1.66)$. Correspondingly, we obtain for $\phi = 0.25$, $\sigma_\psi = 6°$ and $\phi = 0.05$, $\sigma_\psi = 0.06°$ and $\phi = 0.05$, $\sigma_\psi = 6°$ the tupels $(0.52, 2.53)$ and $(0.80, 0.16)$ and $(0.80, 0.35)$, respectively. These values and the results in Fig. 4.7 suggest that (4.38) can indeed be used to predict whether or not BS distortion noise is beneficial.

4.6 Conclusions

In this chapter, we have investigated the impact of hardware impairments such as multiplicative phase noise, additive distortion noise, and amplified receiver noise on the secrecy performance of massive MIMO systems employing MF precoding for downlink data transmission. To mitigate the loss of pilot orthogonality during uplink training if multiple MTs emit pilots concurrently, a generalized pilot design was proposed. Furthermore, to avoid the AN leakage caused by the loss of orthogonality between the user channels and the NS AN precoder if multiple noisy LOs are employed at the BS, a novel G-NS AN precoding scheme was introduced. For the considered system, a lower bound on the achievable ergodic secrecy rate of the users was derived. This bound was used to obtain important insights for system design, including the impact of the pilot sequence design, the AN precoder design, the number of LOs, and the various hardware impairment parameters. The following general conclusions can be drawn: 1) Additive distortion noise at the BS may be beneficial for the secrecy performance especially if little or no AN is injected; 2) all other hardware impairments have a negative impact on the ergodic secrecy rate; 3) despite their susceptibility to pilot contamination in the presence of phase noise, SO pilots are preferable except for the case when the phase noise is very strong; 4) if the number of BS antennas is sufficiently large, the proposed G-NS AN precoder outperforms the conventional NS AN precoder in the presence of phase noise.

Chapter 5

Summary of Thesis and Future Research Topics

In this final chapter, in Section 5.1, we summarize our results and highlight the contributions of this thesis. In Section 5.2, we also propose ideas for future related research.

5.1 Summary of Results

This thesis as a whole has focused on physical layer security for massive MIMO systems. In the following, we briefly review the main results of each chapter.

In Chapter 2, we considered a multi-cell massive MIMO system with MF precoding and AN precoding at the BS for secure downlink transmission in the presence of a multi-antenna passive eavesdropper. For AN precoding, we considered both the conventional NS AN precoding matrix design and a novel random AN precoding matrix design. For both perfect training and pilot contamination, we derived two tight lower bounds on the ergodic secrecy rate and a tight upper bound on the secrecy outage probability. The analytical expressions allowed us to optimize the amount of power allocated to AN precoding and to gain significant insight into the impact of the system parameters on performance. In particular, our results reveal that for the considered multi-cell massive MIMO system with MF precoding (1) AN precoding is necessary to achieve a non-zero ergodic secrecy rate if the user and the eavesdropper experience the same path-loss, (2) secrecy cannot be guaranteed if the eavesdropper has too many antennas, (3) for the case of pilot contamination, the ergodic secrecy rate is only an increasing function of the number of BS antennas if the amount of power allocated to AN precoding is optimized, and (4) the proposed random AN precoding matrix design is a promising low-complexity alternative to the conventional NS AN precoding matrix design.

In Chapter 3, we considered downlink multi-cell massive MIMO systems employing linear data and AN precoding for physical layer security provisioning. We analyzed and compared the achievable ergodic secrecy rate of various conventional data and AN precoders in the presence of pilot contamination. To this end, we also optimized the regularization constants of the selfish and collaborative RCI precoders in the presence of AN and multi-cell interference. In addition, we derived linear POLY data and AN precoders which offer a good compromise between complexity and performance in massive MIMO systems. Interesting findings of this chapter include: 1) Collaborative data precoders outperform selfish designs only in lightly loaded systems where a sufficient number of degrees of freedom for suppressing inter-cell interference and sufficient resources for training are available. 2) Similarly, CNS AN precoding is preferable over SNS AN precoding in lightly loaded systems as it causes less AN leakage to the information-carrying signal, whereas in more heavily loaded systems, CNS AN precoding does not have sufficient degrees of freedom for effectively degrading the eavesdropper channel and SNS AN precoding is preferable. 3) For a large number of eavesdropper antennas, where only small positive secrecy rates are achievable, MF data precoding is always preferable compared to SZF and CZF data precoding. 4) The proposed POLY data and AN precoders approach the performances of the

SRCI data and SNS AN precoders with only a few terms in the respective matrix polynomials and are attractive options for practical implementation.

In Chapter 4, we have investigated the impact of hardware impairments such as multiplicative phase noise, additive distortion noise, and amplified receiver noise on the secrecy performance of massive MIMO systems employing MF precoding for downlink data transmission. To mitigate the loss of pilot orthogonality during uplink training if multiple MTs emit pilots concurrently, a generalized pilot design was proposed. Furthermore, to avoid the AN leakage caused by the loss of orthogonality between the user channels and the NS AN precoder if multiple noisy LOs are employed at the BS, a novel G-NS AN precoding scheme was introduced. For the considered system, a lower bound on the achievable ergodic secrecy rate of the users was derived. This bound was used to obtain important insights for system design, including the impact of the pilot sequence design, the AN precoder design, the number of LOs, and the various hardware impairment parameters. The following general conclusions can be drawn: 1) Additive distortion noise at the BS may be beneficial for the secrecy performance especially if inadequate AN is emitted; 2) all other hardware impairments have a negative impact on the ergodic secrecy rate; 3) despite their susceptibility to pilot contamination in the presence of phase noise, SO pilots are preferable except for the case when the phase noise is very strong; 4) if the number of BS antennas is sufficiently large, the proposed G-NS AN precoder outperforms the conventional NS AN precoder in the presence of phase noise.

5.2 Future Work

In the following, we propose some ideas for further research that are similar to or can be based on the work in this thesis.

5.2.1 Physical Layer Security in Massive MIMO Systems under Constant Envelope Precoding

Equipping large antenna array in massive MIMO systems requires each antenna element and its associated radio-frequency (RF) electronics, e.g. power amplifiers (PAs), to be inexpensive and power-efficient. However, cheaply manufactured PAs are in general non-linear devices, which suffer from linearity issues when processing signals with large amplitude-variations. A per-antenna constant envelope (CE) nonlinear precoding was considered in single-user massive MIMO systems in [21]. It was shown that under the per-antenna CE constraint at the BS transmitter, an equivalent single-input single-output (SISO) model over additive white Gaussian noise (AWGN) is obtained for MISO system where we have a single-user equipped with a single-antenna [21]. When a sufficiently large number of antennas is used, the corresponding achievable rate under a per-antenna CE constraint is close to the capacity of the multiple-input single-output (MISO) channel under an average power constraint in the high-power regime. More recently, the idea of per-antenna CE precoding has been extended to multi-user massive MIMO systems over flat and frequency-selective fading channels [75] [81]. To the best of our knowledge, there is no work considering secure transmission under CE precoding in the presence of multi-antenna eavesdroppers. Therefore, one promising research option is to investigate novel data and AN precoding methods, which jointly satisfy the per-antenna CE constraints, and compare their performance with the secrecy capacity achieving scheme for the average total transmit power constrained channel. Some of the results have been reported in [82].

5.2.2 Physical Layer Security in Massive MIMO Systems with Limited RF-Chain Constraints

When multiple antennas are deployed at the BS in a conventional manner, the complex baseband symbols are tuned for both amplitude and phase. The baseband symbols are then upconverted to the carrier frequency after passing through RF chains, whose outputs are coupled with antenna elements. This implies that each antenna element is supported by one dedicated RF chain, which is far too expensive to deploy in massive MIMO systems due to the large number of antenna elements. On the other hand, the rapid development of circuitry technology enables the high dimensional phase-only RF (or analog) processing. In [83] and [84], analog precoding was considered to achieve full diversity order and near-optimal beamforming performance via iterative algorithms. The authors in [85] have taken into account more practical constraints, including only quantized phase control and finite-precision analog-to-digital (A/D) conversion. In order to further enhance the system performance, related literature [86]-[88] have considered a hybrid approach combining digital and analog preocoding together. More precisely, a low dimensional (limited to the number of RF chains) baseband precoding is employed based on the equivalent channel acquired from the product of the analog RF precoder and the actual channel matrix [87]. However, the problems of how the limited RF-chain constraints will affect the system security and how to design the transmission strategy to enhance the system security with such practical constraints have not been studied before. One foreseeable challenge is that the BS may not possess sufficient spatial dimensions for emitting AN due to the limited number of RF chains. This motivates future research in this direction, and some of the results have been reported in [89].

5.2.3 Physical Layer Security in Massive MIMO Systems against Active Eavesdropping

The contributions covered in this thesis, including the aforementioned two future research options, are based on the assumption that the eavesdroppers always remain passive to hide their existence. Another promising topic is to investigate how massive MIMO systems can combat active eavesdropping. Among multiple active eavesdropping techniques, the *pilot contamination attack* [44] poses the most serious secrecy threat to the TDD based massive MIMO systems. For such attacks, the eavesdropper is able to acquire any training sequences assigned to legitimate MTs, as they are fixed and repeatedly adopted for uplink training. In the training phase, the eavesdropper emits the pilots while all legitimate MTs transmit. As such, the estimates at the BS align with both the legitimate MT's and the eavesdropper's channel. The attack not only reduces the estimation accuracy at the BS, but enhances the eavesdropper's capability to detect his/her desired data signals. It is foreseeable that if the emitting power for the eavesdropper is sufficiently large, the achievable secrecy rate eventually approaches zero. In this scenario, emitting conventional NS based AN is no longer efficient, as the designed AN also lies in the NS of the eavesdropper's channel due to the pilot contamination. In the literature, the authors in [42] proposed several techniques to detect the attack by taking advantage of massive MIMO, while the authors in [57] developed a secret key agreement protocol under pilot contamination attack. Methods for combating such attack in a multi-cell network (pilot contaminated) was reported in [59], based on the assumption that the channel covariance matrix of the eavesdropper is low-rank. A more general combating strategy is essential and of great importance. Besides the pilot contamination attack, the eavesdropper is also able to broadcast jamming signals during the data transmission phase, in order to further reduce the detection capability at the legitimate MTs. Consequently, secure massive MIMO system design under active attacks remains many open problems to solve.

Bibliography

[1] E. G. Larsson, F. Tufvesson, O. Edfors, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014.

[2] F. Rusek, D. Persson, B. K. Lau, E. G. Larsson, T. L. Marzetta, O. Edfors, and F. Tufvesson, "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Proc. Mag.*, vol. 30, no. 1, pp. 40–46, Jan. 2013.

[3] E. G. Larsson, F. Tufvesson, *ICC 2013 tutorial on Massive MIMO*, part I and part II, Jun. 2013.

[4] E. Björnson, E. G. Larsson, T. L. Marzetta, "Massive MIMO: Ten myths and one critical question," *IEEE Commun. Mag.*, Mar. 2015.

[5] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of BS antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.

[6] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1436–1449, Apr. 2013.

[7] J. Hoydis, S. ten Brink, and M. Debbah, "Massive MIMO in UL/DL cellular systems: How many antennas do we need," *IEEE Journal Sel. Areas Commun.*, vol. 31, no. 2, pp. 160–171, Feb. 2013.

[8] J. Jose, A. Ashikhmin, T. L. Marzetta, and S. Vishwanath, "Pilot contamination and precoding in multi-cell TDD systems," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2640–2651, Aug. 2011.

[9] J. L. Massey, "An introduction to contemporary cryptology," *Proc. IEEE*, vol. 76, no. 5, pp. 533–549, May 1988.

[10] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical-layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[11] D. J. Love, R. W. Heath Jr., V. K. N. Lau, D. Gesbert, B. D. Rao, and M. Andrews, "An overview of limited feedback in wireless communication systems,"*IEEE Journal Sel. Areas Commun.*, vol. 26, no. 8, pp. 1341–1365, Oct. 2008.

[12] M. Costa, "Writing on dirty paper," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 439–441, May 1983.

[13] X. Gao, F. Tufvesson, O. Edfors, and F. Rusek, "Measured propagation characteristics for very-large MIMO at 2.6 GHz," in *Proc. 46th Annual Asilomar Conference on Signals, Systems, and Computers*, Pacific Grove, CA, US, pp. 295-299, Nov. 2012.

[14] H. Yang and T. L. Marzetta, "Performance of conjugate and zero-forcing beamforming in large-scale antenna systems," *IEEE Journal Sel. Areas Commun.*, vol. 31, no. 2, pp. 172–179, Feb. 2013.

[15] V. K. Nguyen and J. S. Evans, "Multiuser transmit beamforming via regularized channel inversion: A large system analysis," in *Proc. IEEE Global Communications Conference*, New Orleans, LO, US, pp. 1–4, Dec. 2008.

[16] R. R. Müller and S. Verdu, "Design and analysis of low-complexity interference mitigation on vector channels,"*IEEE Journal on Sel. Areas in Commun.*, vol. 19, no. 8, pp. 1429–1441, Aug. 2001.

[17] R. R. Müller, "Polynomial expansion equalizers for communication via large antenna arrays," in *European Personal Mobile Communications Conference (EPMCC)*, Feb. 2001.

[18] E. Björnson, J. Hoydis, M. Kountouris, and M. Debbah, "Massive MIMO systems with non-ideal hardware: Energy efficiency, estimation, and capacity limits," *IEEE Trans. Inform. Theory*, vol. 60, no. 11, Nov. 2014.

[19] T. Schenk, "RF imperfections in high-rate wireless systems: Impact and digital compensation," New York, NY, US: Springer-Verlag, 2008.

[20] R. Krishnan, M. R. Khanzadi, N. Krishnan, Y. Wu, A. Graell i Amat, T. Eriksson, and R. Schober, "Linear massive MIMO precoders in the presence of phase noise- A large-scale analysis," *IEEE Trans. Vehicular Tech.*, vol. PP, no. 99, pp. 1-1, Jun. 2015.

[21] S. K. Mohammed and E. G. Larsson, "Single-user beamforming in large- scale MISO systems with per-antenna constant-envelope constraints: The doughnut channel," *IEEE Trans. Wireless Commun.*, vol. 11, pp. 3992–4005, Nov. 2012.

[22] E. Björnson, M. Matthaiou, and M. Debbah, "Massive MIMO with non-ideal arbitrary arrays: Hardware scaling laws and circuit-aware design," *IEEE Trans. Wireless Commun.*, vol. 14, no. 8, pp. 4353–4368, Aug. 2015.

[23] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[24] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[25] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, pp. 3831–3842, Jul. 2010.

[26] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inform. Forensics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.

[27] A. Khisti and G. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[28] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[29] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel", *IEEE Trans. Inform. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[30] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inform. Theory.*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[31] D. W. K. Ng, E. S. Lo, and R. Schober, "Multi-objective resource allocation for secure communication in cognitive radio networks with wireless information and power transfer," *IEEE Trans. Veh. Tech.*, vol. 65, no. 5, pp. 3166–3184, May 2016.

[32] D. W. K. Ng and R. Schober, "Secure and green SWIPT in distributed antenna networks with limited backhaul capacity," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5082–5097, Sept. 2015.

[33] H. Wang, C. Wang, and D. W. K. Ng, M. H. Lee, and J. Xiao, "Artificial noise assisted secure transmission under training and feedback," *IEEE Trans. Sig. Proc.*, vol. 63, no. 23, pp. 6285–6298, Dec. 2015.

[34] C. Wang, H. Wang, D. W. K. Ng, X. -G. Xia, and C. Liu, "Joint beamforming and power allocation for security in peer-to-peer relay networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 6, pp. 3280–3293, Jun. 2015.

[35] N. Zhao, F. R. Yu, M. Li, Q. Yan, V. C. M. Leung, "Physical layer security issues in interference alignment (IA)-based wireless networks," *IEEE Commun. Maga.*, to appear, Jun. 2016.

[36] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. Collings, "Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3472–3482, Nov. 2012.

[37] M. Pei, J. Wei, K. -K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 544–549, Feb. 2012.

[38] A. Mukherjee, and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Sig. Proc.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[39] Z. Peng, W. Xu, J. Zhu, H. Zhang, and C. Zhao, "On performance and feedback strategy of secure multiuser communications with MMSE channel estimate," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1602-1616, Feb. 2016.

[40] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Multi-objective optimization for robust power efficiency and secure full-duplex wireless communications systems," submitted to *IEEE Trans. Wireless Commun.*, Sept. 2015.

[41] J. Zhu, W. Xu, and V. K. Bhargava, "Relay precoding in multi-user MIMO channels for physical layer security," in *Proc. IEEE/CIC International Communications Conference in China (ICCC 2014)*, Shanghai, P.R.China, Oct. 2014.

[42] D. Kapetanovic, G. Zheng, F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[43] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems, " *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sept. 2014.

[44] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[45] D. Kapetanovic, G. Zheng, K.-K. Wong, and B. Ottersten, "Detection of pilot contamination attack using random training in massive MIMO," in *Proc. IEEE Intern. Symp. Personal, Indoor and Mobile Radio Commun. (PIMRC)*, pp. 13–18, London, UK, Sept. 2013.

[46] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Maga.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[47] G. Geraci, M. Egan, J. Yuan, A. Razi, and I.B. Collings, "Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3472–3482, Nov. 2012.

[48] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, Jun. 2014.

[49] G. Geraci, J. Yuan, and I. B. Collings, "Large system analysis of linear precoding in MISO broadcast channels with confidential messages,"*IEEE Journal on Sel. Areas in Commun.*, vol. 31, no. 9, pp. 1660–1671, Sept. 2013.

[50] T. Dean and A. Goldsmith, "Physical layer cryptography through massive MIMO," *Proc. IEEE Inform. Theory Workshop*, Sevilla, pp. 1–5, Sept. 2013.

[51] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6854–6868, Dec. 2015.

[52] J. Zhu and W. Xu, "Securing massive MIMO via power scaling," *IEEE Commun. Letters*, vol. 20, no. 5, pp. 1014–1017, May 2016.

[53] H. Wei, D. Wang, X. Hou, Y. Zhu, and J. Zhu, "Secrecy analysis for massive MIMO systems with internal eavesdroppers," in *Proc. IEEE 82nd Vehicular Technology Conference 2015 Fall (VTC'15 Fall)*, pp. 1-5, Boston, MA, Sept. 2015.

[54] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?" *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5135–5146, Sept, 2015.

[55] J. Chen, X. Chen, W. Gerstacker, and D. W. K. Ng, "Resource allocation for a massive MIMO relay aided secure communication," *IEEE Trans. Inform. Forensics and Security*, vol. 11, no. 8, pp. 1700–1711, Aug. 2016.

[56] J. Zhang, C. Yuen, C. -K. Wen, S. Jin, K. -K. Wong, and H. Zhu, "Large system secrecy rate analysis for SWIPT MIMO wiretap channels," *IEEE Trans. Inform. Forensics and Security*, vol. 11, no. 1, pp. 74–85, Jan. 2016.

[57] S. Im, H. Jeon, J. Choi, and J. Ha, "Secret key agreement with large antenna arrays under the pilot contamination attack," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6579–6594, Dec. 2015.

[58] Y. Basciftci, C. Koksal, and A. Ashikhmin, "Securing massive MIMO at the physical layer," available: http://arxiv.org/abs/1505.00396.

[59] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission in the presence of an active eavesdropper," in *Proc. of IEEE International Communications Conference (ICC 2015)*, London, Jun. 2015.

[60] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multi-cell massive MIMO systems," in *Proc. IEEE Global Telecommunications Conference (Globecom 2013) Workshop*, Atlanta, GA, Dec. 2013.

[61] F. Hiai and D. Petz, "The semicircle law, free random variables and entropy," American Mathematical Society, 2006.

[62] J. Zhu, R. Schober, and V. K. Bhargava, "Secure downlink transmission in massive MIMO system with zero-forcing precoding," in *Proc. IEEE European Wireless 2014*, Barcelona, Spain, May 2014.

[63] J. Zhu, R. Schober, and V. K. Bhargava, "Secrecy analysis of multi-cell massive MIMO systems with RCI precoding and artificial noise transmission," in *Proc. IEEE International Symposium on Communications, Control, and Signal Processing 2014 (ISCCSP'14)*, Athens, Greece, May 2014.

[64] J. Zhu, R. Schober, and V. K. Bhargava, "Linear Precoding of Data and Artificial Noise in Secure Massive MIMO Systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.

[65] J. Zhu, R. Schober, and V. K. Bhargava, "Physical layer security for massive MIMO systems impaired by phase noise," submitted to *IEEE International Workshop on Sig. Proc. Advances in Wireless Commun. (SPAWC 2016)*, Feb. 2016. Available: http://arxiv.org/pdf/1603.01869v1.pdf.

[66] J. Zhu, D. W. K. Ng, N. Wang, R. Schober, and V. K. Bhargava, "Analysis and design of secure massive MIMO systems in the presence of hardware impairments," submitted to *IEEE Trans. Wireless Commun.*, Feb. 2016. Available: http://arxiv.org/pdf/1602.08534v1.pdf.

[67] J. Zhang, R. W. Heath Jr., M. Koutouris, and J. G. Andrews, "Mode switching for MIMO broadcast channel based on delay and channel quantization," *EURASIP Journal on Advances in Signal Processing*, vol. 2009, doi:10.1155/2009/802548.

[68] M. Kobayashi, N. Jindal, and G. Caire, "Training and feedback optimization for multiuser MIMO downlink," *IEEE Trans. Commun.*, vol. 59, no. 8, pp. 2228–2240, Aug. 2011.

[69] Q. T. Zhang and D. P. Liu, “A simple capacity formula for correlated diversity Rician channels,” *IEEE Commun. Lett.*, vol. 6, no. 11, pp. 481–483, Nov. 2002.

[70] W. Liao, T. Chang, W. Ma, and C. Chi, “QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach,” *IEEE Trans. Sig. Proc.*, vol. 59, no. 3, pp. 1202–1216, March 2011.

[71] A. Müller, A. Kammoun, E. Björnson, and M. Debbah, “Linear precoding based on polynomial expansion: Reducing complexity in massive MIMO,” arXiv:1310.1806v4 [cs.IT].

[72] A. Kammoun, A. Müller, E. Björnson, and M. Debbah, “Linear precoding based on polynomial expansion: Large-scale multi-cell MIMO Systems,” *IEEE Journal of Sel. Topics in Sig. Proc.*, vol. 8, no. 5, pp. 861–875, Oct. 2014.

[73] S. Zarei, W. Gerstacker, R. R. Muller, and R. Schober, “Low-complexity linear precoding for downlink large-scale MIMO systems,” in *Proc. IEEE Int. Symp. Personal, Indoor and Mobile Radio Commun. (PIMRC)*, Sept. 2013.

[74] R. Hunger, “Floating point operations in matrix-vector calculus,” Technische Universität München, Associate Institute for Signal Processing, Tech. Rep., 2007.

[75] S. K. Mohammed and E. G. Larsson, “Per-antenna constant envelope precoding for large multi-user MIMO systems,”*IEEE Trans. Commun.*, vol. 61, no. 3, pp. 1059–1071, Mar. 2013.

[76] M. Wenk, “MIMO-OFDM testbed: Challenges, implementations, and measurement results (Microelectronics),” Konstanz, Germany: Hartung-Gorre, 2010.

[77] A. Pitarokoilis, S. K. Mohammed, E. G. Larsson, “Uplink performance of time-reversal MRC in massive MIMO systems subject to phase noise,” emphIEEE Trans. Wireless Commun., vol. 14, no. 2, pp. 711–723, Feb. 2015.

[78] Analog Devices, “FR agile transceiver,” AD9364 datasheet, Feb. 2014. [Revised July 2014]

[79] G. Colavolpe, A. Barbieri, and G. Caire, “Algorithms for iterative decoding in the presence of strong phase noise, ” *IEEE J. Sel. Area Commun.*, vol. 23, no. 9, pp. 1748–1757, Sept. 2005.

[80] R. Krishnan, M. R. Khanzadi, T. Eriksson, and T. Svensson, “Soft metrics and their performance analysis for optimal data detection in the presence of strong oscillator phase noise, ” *IEEE Trans. Commun.*, vol. 61, no. 6, pp. 2385–2395, Jun. 2013.

[81] S. K. Mohammed and E. G. Larsson, “Constant-envelope multi-usetr precoding for frequency-selective massive MIMO systems,” *IEEE Wireless Commun. Letters*, vol.2, pp. 547–550, Oct. 2013.

[82] J. Zhu, N. Wang, and V. K. Bhargava, “Per-antenna constant envelope precoding for secure transmission in large-scale MISO systems,” in *Proc. IEEE/CIC International Communications Conference in China (ICCC 2015)*, Shenzhen, P.R.China, Nov. 2015.

[83] D. J. Love and R. W. Heath, Jr. “Equal gain transmission in multipl-input multiple-output wireless systems,” *IEEE Trans. Commun.*, vol. 51, no. 7, pp. 1102–1110, Jul. 2003.

[84] X. Zheng, Y. Xie, J. Li, and P. Stoica, “MIMO transmit beamforming under uniform elemental power constraint,” *IEEE Trans. Sig. Proc.*, vol. 55, no. 11, pp. 5395–5406, Nov. 2007.

[85] V. Venkateswaran and A. J. van der Veen, “Analog beamforming in MIMO communications with phase shift networks and online channel estimation,” *IEEE Trans. Sig. Proc.*, vol. 58, no. 8, pp. 4131–4143, Aug. 2010.

[86] O. E. Ayach, S. Rajagopal, S. Abu-Surra, Z. Pi, and R. W. Heath, Jr., “Spatially sparse precoding in millimeter wave MIMO systems,” *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1499–1513, Mar. 2014.

[87] A. Alkhateeb, O. E. Ayach, G. Leus, and R. W. Heath, Jr., “Channel estimation and hybrid precoding for millimeter wave cellular systems,” *IEEE J. Sel. Topics in Sig. Proc., special issue on Massive MIMO Communication*, vol. 8, no. 5, pp. 831–846, Oct. 2014.

[88] A. Alkhateeb, G. Leus, and R. W. Heath, Jr., “Limited feedback hybrid precoding for multi-user millimeter wave systems,” *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6481–6494, Nov. 2015.

[89] J. Zhu and W. Xu, “Secure massive MIMO systems with limited RF chains,” submitted to *IEEE Trans. Veh. Tech.*, Mar. 2016.

[90] I. Csiszar and J. Körner, “Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[91] D. Tse and P. Viswanath, “Fundemantals of wireless communications,”*Cambridge University Press*, 2005.

[92] H. Gao, P. J. Smith, and M. V. Clark, “Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels,” *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 666–672, May 1998.

[93] A. M. Tulino and S. Verdu, “Random matrix theory and wireless communications, ” *Foundations and Trends in Communications and Information Theory*, vol. 1, no. 1, pp. 1–182, Jun. 2004.

[94] S. W. Nydick, “The Wishart and Inverse Wishart Distributions,” May 2012, [online] http://www.tc.umn.edu/ nydic001/docs/unpubs/Wishart_Distribution.pdf.

[95] J. Evans and D. N. C. Tse, “Large system performance of linear multiuser receivers in multipath fading channels,” *IEEE Trans. Inform. Theory*, vol. 46, no. 6, pp. 2059–2018, Sept. 2000.

Appendix A

Proofs in Chapter 2

Appendix A provides the proofs of Lemmas and Theorems in Chapter 2.

A.1 Proof of Lemma 2.1

The proof closely follows [36]. We first derive an expression for the secrecy rate for given realizations of $\mathbf{h}_{mk}$ and $\mathbf{H}_m^{\text{eve}}$, $k = 1, \ldots, K$, $m = 1, \ldots, M$. Since the MISOME channel in (2.5) and (2.6) is a non-degraded broadcast channel [27], the secrecy capacity is given by [36], [90]

$$C_{nk}^{\text{sec}}(\mathbf{h}) = \max_{s_{nk} \rightarrow \mathbf{w}_{nk} s_{nk} \rightarrow y_{nk}, \mathbf{y}_{\text{eve}}} I\left(s_{nk}; y_{nk} | \mathbf{h}\right) - I\left(s_{nk}; \mathbf{y}_{\text{eve}} | \mathbf{h}\right), \tag{A.1}$$

where vector $\mathbf{h}$ contains the CSI of all user and eavesdropper channels and $I(x; y|\mathbf{h})$ is the mutual information between two r.v.s x and y conditioned on the CSI vector. $C_{nk}^{\text{sec}}(\mathbf{h})$ is achieved by maximizing over all joint distributions such that a Markov chain $s_{nk} \rightarrow \mathbf{w}_{nk} s_{nk} \rightarrow y_{nk}, \mathbf{y}_{\text{eve}}$ results, where s_{nk} is an arbitrary input variable [36]. Specifically, for $s_{nk} \sim \mathbb{CN}(0, 1)$ an achievable secrecy rate for the k^{th} MT in the local cell, $R_{nk}^{\text{sec}}(\mathbf{h})$, is given by

$$\begin{aligned} R_{nk}^{\text{sec}}(\mathbf{h}) &= \Big[I\left(s_{nk}; y_{nk} | \mathbf{h}\right) - I\left(s_{nk}; \mathbf{y}_{\text{eve}} | \mathbf{h}\right) \Big]^{+} \\ &\overset{(a)}{=} \Big[I\left(\mathbf{w}_{nk} s_{nk}; y_{nk} | \mathbf{h}\right) - I\left(\mathbf{w}_{nk} s_{nk}; \mathbf{y}_{\text{eve}} | \mathbf{h}\right) \Big]^{+} \\ &\overset{(b)}{\geq} \Big[R_{nk}\left(\mathbf{h}\right) - C_{nk}^{\text{eve}}\left(\mathbf{h}\right) \Big]^{+} \end{aligned} \tag{A.2}$$

where (a) follows since $\mathbf{w}_{nk} s_{nk}$ is a deterministic function of s_{nk}. Furthermore, $R_{nk}(\mathbf{h}) \leq \max I\left(\mathbf{w}_{nk} s_{nk}; y_{nk} | \mathbf{h}\right)$ is an achievable rate of the k^{th} MT in the local cell and $C_{nk}^{\text{eve}}(\mathbf{h}) = \log_2\left(1 + p \mathbf{w}_{nk}^{H} \mathbf{H}_{n}^{\text{eve}H} \mathbf{X}^{-1} \mathbf{H}_{n}^{\text{eve}} \mathbf{w}_{nk}\right) \geq I\left(\mathbf{w}_{nk} s_{nk}; \mathbf{y}_{\text{eve}} | \mathbf{h}\right)$ is an upper bound on the mutual information $I\left(\mathbf{w}_{nk} s_{nk}; \mathbf{y}_{\text{eve}} | \mathbf{h}\right)$. Thus, follows (b). We note that for computation of $C_{nk}^{\text{eve}}(\mathbf{h})$ we made the worst-case assumption that the eavesdropper can decode and cancel the signals of all MTs except the signal intended for the MT of interest [91, Chapter 10.2].

Finally, to arrive at the ergodic secrecy rate, we average $R_{nk}^{\text{sec}}(\mathbf{h})$ over all channel realizations, which results in [25]

$$\begin{aligned} \mathbb{E}\Big[R_{nk}^{\text{sec}}(\mathbf{h}) \Big] &= \mathbb{E}\Big[\Big[R_{nk}\left(\mathbf{h}\right) - C_{nk}^{\text{eve}}\left(\mathbf{h}\right) \Big]^{+} \Big] \\ &\geq \Big[\mathbb{E}\left[R_{nk}\left(\mathbf{h}\right)\right] - \mathbb{E}\left[C_{nk}^{\text{eve}}\left(\mathbf{h}\right)\right] \Big]^{+} = R_{nk}^{\text{sec}}. \end{aligned} \tag{A.3}$$

Introducing the definitions of the achievable ergodic secrecy rate, $R_{nk} = \mathbb{E}\left[R_{nk}\left(\mathbf{h}\right)\right]$, and the ergodic eavesdropper capacity, $C_{nk}^{\text{eve}} = \mathbb{E}\left[C_{nk}^{\text{eve}}\left(\mathbf{h}\right)\right]$, completes the proof.

A.2 Proof of Theorem 2.1

We first recall that the entries of $\mathbf{H}_m^{\text{eve}}$, $m = 1, \ldots, M$, are mutually independent complex Gaussian r.v.s. On the other hand, for $N_t \to \infty$ and both AN shaping matrix designs, the vectors $\mathbf{v}_{ml}, l = 1, \ldots, N_t - K$, form an orthonormal basis. Hence, $\mathbf{H}_m^{\text{eve}} \mathbf{V}_m$, $m = 1, \ldots, M$, also has independent complex Gaussian entries, which are independent from the complex Gaussian entries of $\mathbf{H}_n^{\text{eve}} \mathbf{w}_{nk}$. Thus, the term $\gamma_{\text{eve}} = p \mathbf{w}_{nk}^H \mathbf{H}_n^{\text{eve}H} \mathbf{X}^{-1} \mathbf{H}_n^{\text{eve}} \mathbf{w}_{nk}$ in (2.8) is equivalent to the SINR of an N_e-branch MMSE diversity combiner with $M(N_t - K)$ interferers [25, 92]. As a result, for the considered simplified path-loss model, the cumulative density function (CDF) of the received SINR, γ_{eve}, at the eavesdropper is given by [92]

$$F_{\gamma_{\text{eve}}}(x) = \frac{\sum_{i=0}^{N_e - 1} \lambda_i x^i}{\prod_{j=1}^{2} (1 + \mu_j x)^{b_j}}, \tag{A.4}$$

where λ_i, μ_j, and b_j are defined in [66, Theorem 1]. Exploiting (A.4), we can rewrite (2.8) as

$$\begin{aligned} C_{\text{eve}} &\overset{(a)}{=} \frac{1}{\ln 2} \int_0^{\infty} (1 + x)^{-1} F_{\gamma_{\text{eve}}}(x) dx \\ &= \frac{1}{\ln 2} \sum_{i=0}^{N_e - 1} \lambda_i \times \int_0^{\infty} \frac{x^i}{(1 + x) \prod_{j=1}^{2} (1 + \mu_j x)^{b_j}} dx \\ &\overset{(b)}{=} \frac{1}{\ln 2} \sum_{i=0}^{N_e - 1} \lambda_i \times \frac{1}{\mu_0} \sum_{j=1}^{2} \sum_{l=1}^{b_j} \int_0^{\infty} \frac{\omega_{jl}}{(x+1)(x + \frac{1}{\mu_j})^l} dx \\ &\overset{(c)}{=} \frac{1}{\ln 2} \sum_{i=0}^{N_e - 1} \lambda_i \times \frac{1}{\mu_0} \sum_{j=1}^{2} \sum_{l=2}^{b_j} \omega_{jl} I(1/\mu_j, l), \end{aligned} \tag{A.5}$$

where μ_0, ω_{jl}, and $I(\cdot, \cdot)$ are defined in Theorem 2.1. Here, (a) is obtained using integration by parts, (b) holds if the order of x in the denominator of (A.4) is not smaller than that in the numerator, i.e., $N_t - K \geq N_e/M$ or equivalently $1-\beta \geq \alpha/M$, which is also the condition to ensure invertibility of $\mathbf{X}$ in (2.8), and (c) is obtained using the definition of $I(\cdot,\cdot)$ given in Theorem 2.1. This completes the proof.

A.3 Proof of Theorem 2.2

Using Jensen's inequality and the mutual independence of $\tilde{\mathbf{w}}_{nk} = \mathbf{H}_n^{\mathrm{eve}}\mathbf{w}_{nk}$ and $\mathbf{H}_m^{\mathrm{eve}}\mathbf{V}_m$, $m = 1, \ldots, M$ (cf. Appendix B), C_{nk}^{eve} in (2.8) is upper bounded by

$$C_{nk}^{\mathrm{eve}} \leq \log_2 \left(1 + \mathbb{E}_{\tilde{\mathbf{w}}_{nk}} \left[p\tilde{\mathbf{w}}_{nk}^H \mathbb{E}\left[\mathbf{X}^{-1}\right] \tilde{\mathbf{w}}_{nk}\right]\right). \tag{A.6}$$

Let us first focus on the term $\mathbb{E}\left[\mathbf{X}^{-1}\right]$ in (A.6) and note that $\mathbf{X}$ is statistically equivalent to a weighted sum of two scaled Wishart matrices [93]. Specifically, we have $\mathbf{X} = q\mathbf{X}_1 + \rho q\mathbf{X}_2$ with $\mathbf{X}_1 \sim \mathcal{W}_{N_e}(N_t - K, \mathbf{I}_{N_e})$ and $\mathbf{X}_2 \sim \mathcal{W}_{N_e}((M-1)(N_t-K), \mathbf{I}_{N_e})$, where $\mathcal{W}_A(B, \mathbf{I}_A)$ denotes an $A \times A$ Wishart matrix with B degrees of freedom. Strictly speaking, $\mathbf{X}$ is not a Wishart matrix, and the exact distribution of $\mathbf{X}$ seems intractable. However, $\mathbf{X}$ may be accurately approximated as a single scaled Wishart matrix, $\mathbf{X} \sim \mathcal{W}_{N_e}(\varphi, \xi\mathbf{I}_{N_e})$, where parameters ξ and φ are chosen such that the first two moments of $\mathbf{X}$ and $q\mathbf{X}_1 + \rho q\mathbf{X}_2$ are identical [69, 94]. Equating the first two moments of the traces of these matrices yields [94]

$$\xi\varphi = q(N_t - K) + \rho q(M-1)(N_t - K), \tag{A.7}$$

and

$$\xi^2\varphi = q^2(N_t - K) + \rho^2 q^2(M-1)(N_t - K). \tag{A.8}$$

By exploiting the expectation of an inverse Wishart matrix given in [94, Eq. (12)], we obtain $\mathbb{E}[\mathbf{X}^{-1}] = \frac{1}{\xi(\varphi - N_e - 1)}\mathbf{I}_{N_e}$ with $\xi = cq/a$ if $\varphi - N_e > 1$ or equivalently if $\beta < 1 - c\alpha/a^2$ for $N_t \to \infty$. Plugging this result and $\mathbb{E}[\tilde{\mathbf{w}}_{nk}^H \tilde{\mathbf{w}}_{nk}] = N_e$ into (A.6), we finally obtain the result in (2.16). This completes the proof.

Appendix B

Proofs in Chapter 3

Appendix B provides the proofs of Propositions, Corollaries, and Theorems in Chapter 3.

B.1 Derivation of $\hat{\mathbf{h}}_{nm}^{k}$ in Section 3.2.2

Let $\sqrt{\tau}\boldsymbol{\omega}_{mk} \in \mathbb{C}^{\tau\times 1}$ be the pilot sequence of length τ transmitted by the k^{th} MT in the m^{th} cell in the training phase, where $\boldsymbol{\omega}_{lj}^{H}\boldsymbol{\omega}_{mk} = 1$, if $l \in \mathcal{M}_m \cup \{m\}$ and $j = k$, and equals zero otherwise, where set $\mathcal{M}_m, \forall m$ is defined in Section 3.2.2. The training signal received at the n^{th} BS, $\mathbf{Y}_n^{\text{pilot}} \in \mathbb{C}^{\tau\times N_T}$ is given in (2.1), with $\boldsymbol{\omega}_{mk}$ instead of $\boldsymbol{\omega}_k$. Assuming MMSE channel estimation [7, 8], the estimate of $\mathbf{h}_{nm}^{k}$ given $\mathbf{Y}_n^{\text{pilot}}$ can be derived as

$$\begin{aligned}
\hat{\mathbf{h}}_{nm}^{k} &= \sqrt{p_\tau \tau \beta_{nm}^{k}}\boldsymbol{\omega}_{mk}^{H}\left(\mathbf{I}_\tau + p_\tau \tau \sum_{l=1}^{M}\sum_{j=1}^{K}\boldsymbol{\omega}_{lj}\beta_{nl}^{j}\boldsymbol{\omega}_{lj}^{H}\right)^{-1}\mathbf{Y}_n^{\text{pilot}} \\
&= \sqrt{p_\tau \tau \beta_{nm}^{k}}\boldsymbol{\omega}_{mk}^{H}\left(\mathbf{I}_\tau + \mathbf{A}_{mk} + \mathbf{B}_{mk}\right)^{-1}\mathbf{Y}_n^{\text{pilot}} \\
&\overset{(a)}{=} \sqrt{p_\tau \tau \beta_{nm}^{k}}\boldsymbol{\omega}_{mk}^{H}\left(\left(\mathbf{I}_\tau + \mathbf{A}_{mk}\right)\left(\mathbf{I}_\tau + \mathbf{B}_{mk}\right)\right)^{-1}\mathbf{Y}_n^{\text{pilot}} \\
&= \sqrt{p_\tau \tau \beta_{nm}^{k}}\boldsymbol{\omega}_{mk}^{H}\left(\mathbf{I}_\tau + \mathbf{B}_{mk}\right)^{-1}\left(\mathbf{I}_\tau + \mathbf{A}_{mk}\right)^{-1}\mathbf{Y}_n^{\text{pilot}} \\
&= \sqrt{p_\tau \tau \beta_{nm}^{k}}\boldsymbol{\omega}_{mk}^{H}\left(\mathbf{I}_\tau - \mathbf{B}_{mk}\left(\mathbf{I}_\tau + \mathbf{B}_{mk}\right)^{-1}\right)\left(\mathbf{I}_\tau + \mathbf{A}_{mk}\right)^{-1}\mathbf{Y}_n^{\text{pilot}} \\
&\overset{(b)}{=} \sqrt{p_\tau \tau \beta_{nm}^{k}}\boldsymbol{\omega}_{mk}^{H}\left(\mathbf{I}_\tau + \mathbf{A}_{mk}\right)^{-1}\mathbf{Y}_n^{\text{pilot}} \\
&= \frac{\sqrt{p_\tau \tau \beta_{nm}^{k}}}{1 + p_\tau \tau \beta_{nm}^{k} + p_\tau \tau \sum_{l\in\mathcal{M}_m}\beta_{nl}^{k}}\boldsymbol{\omega}_{mk}^{H}\mathbf{Y}_n^{\text{pilot}}. \qquad \text{(B.1)}
\end{aligned}$$

where

$$\mathbf{A}_{mk} = p_\tau \tau \sum_{l \in \mathcal{M}_m \cup \{m\}} \boldsymbol{\omega}_{lk} \beta_{nl}^{k} \boldsymbol{\omega}_{lk}^{H} \in \mathbb{C}^{\tau \times \tau}, \tag{B.2}$$

and

$$\mathbf{B}_{mk} = p_\tau \tau \sum_{l \in \mathcal{M}_m \cup \{m\}} \sum_{j \neq k} \boldsymbol{\omega}_{lj} \beta_{nl}^{j} \boldsymbol{\omega}_{lj}^{H} + p_\tau \tau \sum_{l \notin \mathcal{M}_m \cup \{m\}} \sum_{j=1}^{K} \boldsymbol{\omega}_{lj} \beta_{nl}^{j} \boldsymbol{\omega}_{lj}^{H} \in \mathbb{C}^{\tau \times \tau}. \tag{B.3}$$

In (B.1), (a) is due to $\mathbf{A}_{mk}\mathbf{B}_{mk} = \mathbf{0}$, while (b) uses $\boldsymbol{\omega}_{mk}^{H}\mathbf{B}_{mk} = \mathbf{0}$. For the special case of $\mathcal{M}_m = \mathcal{M}\backslash\{m\}$, (B.1) reduces to (2.2) in Chapter 2 with n instead of m when estimating the in-cell CSI.

B.2 Proof of Proposition 3.1

Considering (3.3) and (3.10), the effective signal power, i.e., the numerator in (3.6), can be expressed as [15]

$$\mathbb{E}^2[\mathbf{h}_{nn}^{k}\mathbf{f}_{nk}] = \gamma_1^2 \mathbb{E}^2[\mathbf{h}_{nn}^{k}\mathbf{L}_{nn}(\hat{\mathbf{h}}_{nn}^{k})^H] = \gamma_1^2 \mathbb{E}^2\left[\frac{\mathbf{h}_{nn}^{k}\mathbf{L}_{n,k}(\hat{\mathbf{h}}_{nn}^{k})^H}{1+\hat{\mathbf{h}}_{nn}^{k}\mathbf{L}_{n,k}(\hat{\mathbf{h}}_{nn}^{k})^H}\right] = \frac{\gamma_1^2 \lambda_{nk}(X_{nk}+A_{nk})^2}{\beta_{nn}^{k}(1+X_{nk})^2}, \tag{B.4}$$

where $\mathbf{L}_{n,k} = (\hat{\mathbf{H}}_{nn}\hat{\mathbf{H}}_{nn}^{H} - (\hat{\mathbf{h}}_{nn}^{k})^H\hat{\mathbf{h}}_{nn}^{k} + \kappa_1 \mathbf{I}_{N_T})^{-1}$, $X_{nk} = \mathbb{E}[\hat{\mathbf{h}}_{nn}^{k}\mathbf{L}_{n,k}(\hat{\mathbf{h}}_{nn}^{k})^H]$, and $A_{nk} = \mathbb{E}[\tilde{\mathbf{h}}_{nn}^{k}\mathbf{L}_{n,k}(\hat{\mathbf{h}}_{nn}^{k})^H]$. On the other hand, the intra-cell interference term in the denominator of (3.6) can be expressed as

$$\mathbb{E}\left[\sum_{l \neq k} |\mathbf{h}_{nn}^{k}\mathbf{f}_{nl}|^2\right] = \gamma_1^2 \mathbb{E}\left[\frac{\mathbf{h}_{nn}^{k}\mathbf{L}_{n,k}\hat{\mathbf{H}}_{n,k}^{H}\hat{\mathbf{H}}_{n,k}\mathbf{L}_{n,k}(\mathbf{h}_{nn}^{k})^H}{\left(1+\hat{\mathbf{h}}_{nn}^{k}\mathbf{L}_{n,k}(\hat{\mathbf{h}}_{nn}^{k})^H\right)^2}\right] = \frac{\gamma_1^2 \lambda_{nk}(Y_{nk}+B_{nk})}{\beta_{nn}^{k}(1+X)^2}, \tag{B.5}$$

where $\hat{\mathbf{H}}_{n,k}$ is equal to $\hat{\mathbf{H}}_{nn}$ with the k^{th} row removed, and

$$Y_{nk} = \mathbb{E}[\hat{\mathbf{h}}_{nn}^{k}\mathbf{L}_{n,k}\hat{\mathbf{H}}_{n,k}^{H}\hat{\mathbf{H}}_{n,k}\mathbf{L}_{n,k}(\hat{\mathbf{h}}_{nn}^{k})^{H}], \quad B_{nk} = \mathbb{E}[\tilde{\mathbf{h}}_{nn}^{k}\mathbf{L}_{n,k}\hat{\mathbf{H}}_{n,k}^{H}\hat{\mathbf{H}}_{n,k}\mathbf{L}_{n,k}(\tilde{\mathbf{h}}_{nn}^{k})^{H}]. \tag{B.6}$$

Due to pilot contamination, the data precoding matrix of the m^{th} BS is a function of the channel vectors between the m^{th} BS and the MTs in all cells with reused pilots. Hence, the inter-cell interference from the the m^{th} BS (if $m \in \mathcal{M}_n$) is obtained as

$$\mathbb{E}[|\mathbf{h}_{mn}^{k}\mathbf{f}_{mk}|^2] = \frac{\gamma_1^2\lambda_{mk}(X_{mk}+A_{mk})^2}{\beta_{mn}^{k}(1+X_{mk})^2} + \frac{\theta_{mn}^{k}}{\theta_{mn}^{k}+p_\tau\tau\beta_{mn}^{k}} \tag{B.7}$$

and

$$\mathbb{E}\left[\sum_{l\neq k}|\mathbf{h}_{mn}^{k}\mathbf{f}_{ml}|^2\right] = \gamma_1^2\mathbb{E}\left[\frac{\mathbf{h}_{mn}^{k}\mathbf{L}_{m,k}\hat{\mathbf{H}}_{m,k}^{H}\hat{\mathbf{H}}_{m,k}\mathbf{L}_{m,k}(\mathbf{h}_{mn}^{k})^{H}}{\left(1+\hat{\mathbf{h}}_{mm}^{k}\mathbf{L}_{m,k}(\hat{\mathbf{h}}_{mm}^{k})^{H}\right)^2}\right] = \frac{\gamma_1^2\lambda_{mk}(Y_{mk}+B_{mk})}{\beta_{mn}^{k}(1+X_{mk})^2}, \tag{B.8}$$

respectively. Meanwhile, by exploiting (B.4), (B.7), and the definition of the variance, i.e., $\text{var}[x] = \mathbb{E}[x^2] - \mathbb{E}^2[x]$, we obtain for the first term of the denominator of (3.6)

$$\text{var}[\mathbf{h}_{nn}^{k}\mathbf{f}_{nk}] = \frac{\theta_{nn}^{k}}{\theta_{nn}^{k}+p_\tau\tau\beta_{nn}^{k}}. \tag{B.9}$$

According to [15, Eq. (16)] and [95, Theorem 7], for $N_T \to \infty$ and constant β, X_{mk} converges to $\mathcal{G}(\beta,\kappa_1)$ defined in (3.12) and $A_{mk} \to 0$. Similarly, Y_{mk} and B_{mk} approach

$$Y_{mk} \overset{N_T\to\infty}{=} \mathcal{G}(\beta,\kappa_1) + \kappa_1\frac{\partial}{\partial\kappa_1}\mathcal{G}(\beta,\kappa_1) \tag{B.10}$$

and

$$B_{mk} \overset{N_T\to\infty}{=} \frac{\mu_{mk}}{\lambda_{mk}}(1+\mathcal{G}(\beta,\kappa_1))^2\left(\mathcal{G}(\beta,\kappa_1) + \kappa_1\frac{\partial}{\partial\kappa_1}\mathcal{G}(\beta,\kappa_1)\right), \tag{B.11}$$

respectively, where $\frac{\partial}{\partial \kappa_1}\mathcal{G}(\beta, \kappa_1) = -\frac{\mathcal{G}(\beta,\kappa_1)(1+\mathcal{G}(\beta,\kappa_1))^2}{\beta+\kappa_1(1+\mathcal{G}(\beta,\kappa_1))^2}$.

Moreover, the inter-cell interference from other non-contaminated cells (i.e., $m \notin \mathcal{M}_n \bigcup \{n\}$) is calculated as

$$\mathbb{E}\Big[\mathbf{h}_{mn}^k \mathbf{F}_{m,k} \mathbf{F}_{m,k}^H (\mathbf{h}_{mn}^k)^H\Big] = \mathbb{E}\Big[\mathrm{tr}\left\{\mathbf{F}_{m,k}\mathbf{F}_{m,k}^H\right\}\Big] = K - 1, \qquad \text{(B.12)}$$

where $\mathbf{F}_{m,k}$ is equal to $\mathbf{F}_m$ with the k^{th} column removed. The first equality in (B.12) is due to the fact that the precoding matrix for the other MTs (i.e., not the k^{th} MTs) in adjacent cells are independent of $\mathbf{h}_{mn}^k$ and [71, Lemma 11], while the second equality holds for $N_T \to \infty$.

On the other hand, the constant scaling factor γ_1 for SRCI precoding is given by [15, Eq. (22)]

$$\gamma_1^2 = \frac{\phi P}{\mathcal{G}(\beta, \kappa_1) + \kappa_1 \frac{\partial}{\partial \kappa_1}\mathcal{G}(\beta, \kappa_1)}. \qquad \text{(B.13)}$$

Hence, employing (B.4)-(B.13) in (3.6), the received SINR in (3.11) is obtained as $\gamma_{nk}^{\text{SRCI}}$

$$\begin{aligned}
&= \frac{\frac{\gamma_1^2 \lambda_{nk} X_{nk}^2}{(1+X_{nk})^2}}{\frac{\gamma_1^2 \sum_{m\in\mathcal{M}_n\cup\{n\}} \lambda_{mk}(Y_{mk}+B_{mk})}{(1+X_{mk})^2} + \sum_{m\in\mathcal{M}_n} \frac{\gamma_1^2 \lambda_{mk} X_{mk}^2}{(1+X_{mk})^2} + p\sum_{m\notin\mathcal{M}_n\cup\{n\}} \sum_{l=1}^K \beta_{mn}^k + qQ + 1} \\
&= \frac{\frac{K\lambda_{nk}}{g+\kappa_1 \frac{\partial g}{\partial \kappa_1}} \frac{g^2}{(1+g)^2}}{K\sum_{m\in\mathcal{M}_n\cup\{n\}} \lambda_{mk} \left(\frac{1+\frac{\mu_{mk}}{\lambda_{mk}}(1+g)^2}{(1+g)^2}\right) + \sum_{m\in\mathcal{M}_n} \frac{\gamma_1^2 \lambda_{mk} g^2}{(1+g)^2 p} + \sigma_1^2} \\
&= \frac{\hat{\Gamma}_{\text{SRCI}}^n g^2}{\left(g + \kappa_1 \frac{\partial g}{\partial \kappa_1}\right)\left(\sum_{m\in\mathcal{M}_n\cup\{n\}} \hat{\Gamma}_{\text{SRCI}}^m + (1+g)^2\right) + \sum_{m\in\mathcal{M}_n} \hat{\Gamma}_{\text{SRCI}}^m g^2} \\
&= \frac{1}{\frac{\left(g+\kappa_1 \frac{\partial}{\partial\kappa_1} g\right)\left(\sum_{m\in\mathcal{M}_n\cup\{n\}} \hat{\Gamma}_{\text{SRCI}}^m + (1+g)^2\right)}{\hat{\Gamma}_{\text{SRCI}}^n g^2} + \sum_{m\in\mathcal{M}_n} \hat{\Gamma}_{\text{SRCI}}^m / \hat{\Gamma}_{\text{SRCI}}^n} \\
&= \frac{1}{\frac{\sum_{m\in\mathcal{M}_n\cup\{n\}} \hat{\Gamma}_{\text{SRCI}}^m + (1+g)^2}{g\left(\hat{\Gamma}_{\text{SRCI}}^n + \frac{\hat{\Gamma}_{\text{SRCI}}^n \kappa_1}{\beta}(1+g)^2\right)} + \sum_{m\in\mathcal{M}_n} \lambda_{mk}/\lambda_{nk}}, \qquad \text{(B.14)}
\end{aligned}$$

where we denote $g = \mathcal{G}(\beta, \kappa_1)$ for notational simplicity, $\sigma_1^2 = \sum_{m \notin \mathcal{M}_n \bigcup \{n\}} \sum_{l=1}^{K} \beta_{mn}^{k} + \eta Q + \frac{K}{\phi P_T}$ and $\hat{\Gamma}_{\text{SRCI}}^{m}$ is defined in Proposition 3.1. This completes the proof.

B.3 Derivation of $\kappa_{1,\text{opt}}$

We first denote $\gamma_{nk}^{\text{SRCI}} = \frac{1}{1/\Gamma + \sum_{m \in \mathcal{M}_n} \lambda_{mk}/\lambda_{nk}}$ in (3.11), where

$$\Gamma = \frac{\hat{\Gamma}_{\text{SRCI}}^{n}}{\beta} \cdot \mathcal{G}(\beta, \kappa_1) \cdot \frac{\beta + \kappa_1 (1 + \mathcal{G}(\beta, \kappa_1))^2}{\Upsilon + (1 + \mathcal{G}(\beta, \kappa_1))^2}. \tag{B.15}$$

with $\Upsilon = \sum_{m \in \mathcal{M}_n \cup \{n\}} \hat{\Gamma}_{\text{SRCI}}^{m}$. From (B.15), it is obvious that the optimal κ_1 to maximize $\gamma_{nk}^{\text{SRCI}}$ is equivalent to the one that maximizes Γ.

In order to obtain the optimal $\kappa_{1,\text{opt}}$, we need the following steps:

$$\begin{aligned} \frac{\partial \Gamma}{\partial \kappa_1} &= \frac{\hat{\Gamma}_{\text{SRCI}}^{n}}{\beta} \left(\frac{\partial g}{\partial \kappa_1} \cdot \frac{\beta + (1+g)^2}{\Upsilon + (1+g)^2} + g \cdot \frac{\partial}{\partial \kappa_1} \left(\frac{\beta + (1+g)^2}{\Upsilon + (1+g)^2} \right) \right) \\ &= \frac{\hat{\Gamma}_{\text{SRCI}}^{n} g}{\beta} \cdot \frac{\beta + (1+g)^2}{\Upsilon + (1+g)^2} \left(\frac{2\kappa_1 (1+g) \partial g / \partial \kappa_1}{\beta + \kappa_1 (1+g)^2} + \frac{2(1+g) \partial g / \partial \kappa_1}{\Upsilon + (1+g)^2} \right) \\ &= \frac{2\Upsilon^2 g (1+g)^2}{\beta \left(\Upsilon + (1+g)^2 \right)^2} \frac{\partial g}{\partial \kappa_1} \left(\kappa_1 - \frac{\beta}{\Upsilon} \right) = 0, \end{aligned} \tag{B.16}$$

where we denote $g = \mathcal{G}(\beta, \kappa_1)$. This finally gives $\kappa_{1,\text{opt}} = \beta / \Upsilon$, which completes the derivation.

B.4 Proof of Corollary 3.1

γ_{nk}^{SZF} in (3.16) can be obtained from (3.11) as $\gamma_{nk}^{\text{SZF}} = \lim_{\kappa_1 \to 0} \gamma_{nk}^{\text{SRCI}}$. In particular, when $\kappa_1 \to 0$, $\mathcal{G}(\beta, \kappa_1)$ in (3.12) can be rewritten as

$$\mathcal{G}(\beta, \kappa_1) = \frac{1}{2\kappa_1} \left(\sqrt{(1-\beta)^2 + 2(1+\beta)\kappa_1 + \kappa_1^2} + (1-\beta) - \kappa_1 \right). \tag{B.17}$$

Plugging this into (B.15), we have

$$\begin{aligned}\Gamma &= \frac{\hat{\Gamma}^n_{\text{SRCI}}}{2\beta}\frac{\left(\sqrt{(1-\beta)^2+2(1+\beta)\kappa_1+\kappa_1^2}+(1-\beta)-\kappa_1\right)}{4\sum_{m\in\mathcal{M}_n\cup\{n\}}\hat{\Gamma}^m_{\text{SRCI}}\kappa_1^2+\left(\sqrt{(1-\beta)^2+2(1+\beta)\kappa_1+\kappa_1^2}+(1-\beta)+\kappa_1\right)^2}\\ &\times\ \left[4\beta\kappa_1+\left(\sqrt{(1-\beta)^2+2(1+\beta)\kappa_1+\kappa_1^2}+(1-\beta)-\kappa_1\right)^2\right],\end{aligned}\tag{B.18}$$

For $\kappa_1\to 0$, we simply have

$$\lim_{\kappa_1\to 0}\gamma^{\text{SRCI}}_{nk}=\frac{1}{\frac{\beta}{(1-\beta)\hat{\Gamma}^n_{\text{SRCI}}}+\sum_{m\in\mathcal{M}_n}\lambda_{mk}/\lambda_{nk}}.\tag{B.19}$$

This completes the proof of Corollary 3.1.

B.5 Proof of Theorem 3.1

The objective function in (3.23) can be rewritten as

$$\begin{aligned}\text{mse}_n &= \varsigma^2 p\mathbb{E}\left[\text{Tr}\left\{\sum_{i=0}^{\mathcal{I}}\mu_i\left(\hat{\bar{\mathbf{H}}}_{nn}\hat{\bar{\mathbf{H}}}^H_{nn}\right)^{i+1}\mathbf{D}_{nn}\sum_{i=0}^{\mathcal{I}}\mu_i\left(\hat{\bar{\mathbf{H}}}_{nn}\hat{\bar{\mathbf{H}}}^H_{nn}\right)^{i+1}\right\}\right]\\ &+\ \varsigma^2 p\mathbb{E}\left[\text{Tr}\left\{\sum_{i=0}^{\mathcal{I}}\mu_i\left(\hat{\bar{\mathbf{H}}}_{nn}\hat{\bar{\mathbf{H}}}^H_{nn}\right)^{i}\hat{\bar{\mathbf{H}}}_{nn}\tilde{\bar{\mathbf{H}}}^H_{nn}\mathbf{D}_{nn}\tilde{\bar{\mathbf{H}}}_{nn}\hat{\bar{\mathbf{H}}}^H_{nn}\sum_{i=0}^{\mathcal{I}}\mu_i\left(\hat{\bar{\mathbf{H}}}_{nn}\hat{\bar{\mathbf{H}}}^H_{nn}\right)^{i}\right\}\right]\\ &-\ 2\varsigma\sqrt{p}\mathbb{E}\left[\text{Tr}\left\{\mathbf{D}^{1/2}_{nn}\sum_{i=0}^{\mathcal{I}}\mu_i\left(\hat{\bar{\mathbf{H}}}_{nn}\hat{\bar{\mathbf{H}}}^H_{nn}\right)^{i+1}\right\}\right]+1+\varsigma^2P_{\text{AN}}+\varsigma^2\text{Tr}\left\{\mathbf{\Sigma}_n\right\},\end{aligned}\tag{B.20}$$

where we exploited $\mathbb{E}[\mathbf{s}_n\mathbf{s}_n^H]=\mathbf{I}_K$, the definition of P_{AN} given in Theorem 3.1, the definition of $\mathbf{F}_n$ in (3.21), the definition $\frac{1}{\sqrt{N_T}}\mathbf{H}_{nn}=\hat{\bar{\mathbf{H}}}_{nn}+\tilde{\bar{\mathbf{H}}}_{nn}$, and $\tilde{\bar{\mathbf{H}}}_{nn}=\frac{1}{\sqrt{N_T}}\tilde{\mathbf{H}}_{nn}$.

In the following, we simplify the right hand side (RHS) of (B.20) term by term. To this end, we denote the first three terms on the RHS of (B.20) by t_1, t_2, and t_3, respectively. Using a result from free probability theory [61], the first term converges to [66, Theorem 1]

$$t_1 = \varsigma^2 p \mathrm{Tr}\left\{\mathbf{D}_{nn}\right\} \mathbb{E}\left[\mathrm{Tr}\left\{\left(\sum_{i=0}^{\mathcal{I}} \mu_i \left(\hat{\bar{\mathbf{H}}}_{nn}\hat{\bar{\mathbf{H}}}_{nn}^H\right)^{i+1}\right)^2\right\}\right], \tag{B.21}$$

as matrix $\mathbf{D}_{nn}$ is free from $\sum_{i=0}^{\mathcal{I}} \mu_i \left(\hat{\bar{\mathbf{H}}}_{nn}\hat{\bar{\mathbf{H}}}_{nn}^H\right)^{i+1}$. Similarly, the third term converges to

$$t_3 = -2\varsigma\sqrt{p}\mathrm{Tr}\left\{\mathbf{D}_{nn}^{1/2}\right\} \mathbb{E}\left[\mathrm{Tr}\left\{\sum_{i=0}^{\mathcal{I}} \mu_i \left(\hat{\bar{\mathbf{H}}}_{nn}\hat{\bar{\mathbf{H}}}_{nn}^H\right)^{i+1}\right\}\right]. \tag{B.22}$$

Furthermore, the second term can be rewritten as

$$\begin{aligned} t_2 &\overset{(a)}{=} \varsigma^2 p \mathbb{E}\left[\mathrm{Tr}\left\{\tilde{\bar{\mathbf{H}}}_{nn}^H \mathbf{D}_{nn} \tilde{\bar{\mathbf{H}}}_{nn}\right\} \mathrm{Tr}\left\{\sum_{i=0}^{\mathcal{I}} \mu_i \left(\hat{\bar{\mathbf{H}}}_{nn}\hat{\bar{\mathbf{H}}}_{nn}^H\right)^{i} \hat{\bar{\mathbf{H}}}_{nn}\hat{\bar{\mathbf{H}}}_{nn}^H \sum_{i=0}^{\mathcal{I}} \mu_i \left(\hat{\bar{\mathbf{H}}}_{nn}\hat{\bar{\mathbf{H}}}_{nn}^H\right)^{i}\right\}\right] \\ &\overset{(b)}{=} \varsigma^2 p N_T \mathrm{Tr}\left\{\mathbf{D}_{nn}\boldsymbol{\Delta}_n\right\}, \end{aligned} \tag{B.23}$$

where (a) follows again from [66, Theorem 1] and (b) results from $\mathbb{E}[\mathrm{Tr}\{\tilde{\bar{\mathbf{H}}}_{nn}^H \mathbf{D}_{nn} \tilde{\bar{\mathbf{H}}}_{nn}\}] = \mathrm{Tr}\left\{\mathbf{D}_{nn}\boldsymbol{\Delta}_n\right\}$, where $\boldsymbol{\Delta}_n$ is defined in Theorem 3.1, (3.21), and the constraint in (3.23).

Exploiting (B.21)-(B.23) and the eigen-decomposition of matrix $\hat{\bar{\mathbf{H}}}_{nn}\hat{\bar{\mathbf{H}}}_{nn}^H = \mathbf{T}\boldsymbol{\Lambda}\mathbf{T}^H$, where diagonal matrix $\boldsymbol{\Lambda} = \mathrm{diag}\left(\lambda_1, \ldots, \lambda_K\right)$ contains all eigenvalues and unitary matrix $\mathbf{T}$ contains the corresponding eigenvectors, the asymptotic average MSE becomes

$$\begin{aligned} \mathrm{mse}_n \;=\; & \mathbb{E}\left[\varsigma^2 p \mathrm{Tr}\left\{\mathbf{D}_{nn}\right\} \mathrm{Tr}\left\{\boldsymbol{\Lambda}^2 \left(\sum_{i=0}^{\mathcal{I}} \mu_i \boldsymbol{\Lambda}^i\right)^2\right\} - 2\varsigma\sqrt{p}\mathrm{Tr}\left\{\mathbf{D}_{nn}^{1/2}\right\} \mathrm{Tr}\left\{\sum_{i=0}^{\mathcal{I}} \mu_i \boldsymbol{\Lambda}^{i+1}\right\}\right] \\ & +1 + \varsigma^2 P_{\mathrm{AN}} + \varsigma^2 \mathrm{Tr}\left\{\boldsymbol{\Sigma}_n\right\} + \varsigma^2 p N_T \mathrm{Tr}\left\{\mathbf{D}_{nn}\boldsymbol{\Delta}_n\right\}. \end{aligned} \tag{B.24}$$

Next, we introduce the Vandermonde matrix $\mathbf{C}_1 \in \mathbb{R}^{K\times(\mathcal{I}+1)}$, where $[\mathbf{C}_1]_{i,j} = \lambda_i^{j-1}$, and $\boldsymbol{\lambda} = [\lambda_1, \ldots, \lambda_K]^T$, which allows us to rewrite (B.24) in compact form as

$$\begin{aligned}\mathrm{mse}_n &= \lim_{K\to\infty} \frac{1}{K}\mathbb{E}\Big[\varsigma^2 p \mathrm{Tr}\left\{\mathbf{D}_{nn}\right\} \boldsymbol{\mu}^T \mathbf{C}_1^T \boldsymbol{\Lambda}^2 \mathbf{C}_1 \boldsymbol{\mu} - 2\varsigma\sqrt{p}\mathrm{Tr}\left\{\mathbf{D}_{nn}^{1/2}\right\} \boldsymbol{\mu}^T \mathbf{C}_1^T \boldsymbol{\lambda}\Big] \\ &\quad +1 + \varsigma^2 P_{\mathrm{AN}} + \varsigma^2 \mathrm{Tr}\left\{\boldsymbol{\Sigma}_n\right\} + \varsigma^2 p N_T \mathrm{Tr}\left\{\mathbf{D}_{nn}\boldsymbol{\Delta}_n\right\}. \qquad \text{(B.25)}\end{aligned}$$

Similarly, the constraint in (3.23) can be expressed as

$$\lim_{K\to\infty} \frac{1}{K}\mathbb{E}\Big[\boldsymbol{\mu}^T \mathbf{C}_1^T \boldsymbol{\Lambda} \mathbf{C}_1 \boldsymbol{\mu}\Big] = N_T. \qquad \text{(B.26)}$$

Thus, the Lagrangian function of primal problem (3.23) can be expressed as $\mathcal{L}_1(\boldsymbol{\mu}, \varsigma) = \mathrm{mse}_n + \epsilon_1(\lim_{K\to\infty} \frac{1}{K}\mathbb{E}[\boldsymbol{\mu}^T \mathbf{C}_1^T \boldsymbol{\Lambda} \mathbf{C}_1 \boldsymbol{\mu}] - N_T)$, where ϵ_1 is the Lagrangian multiplier. Taking the gradient of the Lagrangian function with respect to $\boldsymbol{\mu}$, and setting the result to zero, we obtain for the optimal coefficient vector $\boldsymbol{\mu}_{\mathrm{opt}}$:

$$\lim_{K\to\infty} \frac{1}{K}\mathbb{E}\left[\mathbf{C}_1^T \boldsymbol{\Lambda}\left(\boldsymbol{\Lambda} + \frac{\epsilon_1}{\mathrm{Tr}\left\{\mathbf{D}_{nn}\right\}\varsigma^2 p}\mathbf{I}_K\right)\mathbf{C}_1\right]\boldsymbol{\mu} = \frac{\mathrm{Tr}\left\{\mathbf{D}_{nn}^{1/2}\right\}}{\varsigma\sqrt{p}\mathrm{Tr}\left\{\mathbf{D}_{nn}\right\}} \lim_{K\to\infty} \frac{1}{K}\mathbb{E}\left[\mathbf{C}_1^T \boldsymbol{\lambda}\right]. \qquad \text{(B.27)}$$

Furthermore, taking the derivative of $\mathcal{L}_1(\boldsymbol{\mu}, \varsigma)$ with respect to ς and equating it to zero, and multiplying both sides of (B.27) by $\boldsymbol{\mu}^T$ and applying (B.26), we obtain

$$\frac{\epsilon_1}{\varsigma^2 p} = \mathrm{Tr}\left\{\mathbf{D}_{nn}\boldsymbol{\Delta}_n\right\} + \frac{P_{\mathrm{AN}} + \mathrm{Tr}\left\{\boldsymbol{\Sigma}_n\right\}}{N_T p}. \qquad \text{(B.28)}$$

The expressions involving $\mathbf{C}_1$, $\boldsymbol{\Lambda}$, and $\boldsymbol{\lambda}$ in (B.27) can be further simplified. For example, we obtain $\lim_{K\to\infty}\mathbb{E}\left[\frac{1}{K}\left[\mathbf{C}_1^T\boldsymbol{\Lambda}\mathbf{C}_1\right]_{m,n}\right] = \lim_{K\to\infty}\mathbb{E}\left[\frac{1}{K}\sum_{k=1}^{K}\lambda_k^{m+n-1}\right]$. Simplifying the other terms in (B.27) in a similar manner and inserting (B.28) into (B.27) we obtain the result in Theorem 3.1.

B.6 Proof of Theorem 3.2

Exploiting $\mathbb{E}[\mathbf{z}_n\mathbf{z}_n^H] = \mathbf{I}_{N_T}$, the constraint in (3.33), and a similar approach as was used to arrive at (3.28), the objective function in (3.33) can be rewritten as $P_{\mathrm{AN}} =$

$$q\mathbb{E}\Big[\mathrm{Tr}\left\{\mathbf{G}_{nn}\mathbf{A}_n\mathbf{A}_n^H\mathbf{G}_{nn}^H\right\}\Big] = q\mathbb{E}\Big[\mathrm{Tr}\Big\{\mathbf{D}_{nn}\hat{\mathbf{H}}_{nn}\mathbf{A}_n\mathbf{A}_n^H\hat{\mathbf{H}}_{nn}^H\Big\}\Big] + (1-\phi)P_T\mathrm{Tr}\{\mathbf{D}_{nn}\boldsymbol{\Delta}_n\}. \tag{B.29}$$

Using (3.32) and a similar approach as in Appendix B.5, (B.29) can be rewritten as

$$\begin{aligned} P_{\mathrm{AN}} &= (1-\phi)P_T\mathrm{Tr}\{\mathbf{D}_{nn}\boldsymbol{\Delta}_n\} \\ &+ qN_T\mathrm{Tr}\left\{\mathbf{D}_{nn}\right\}\mathbb{E}\Bigg[-2\mathrm{Tr}\bigg\{\sum_{j=0}^{\mathcal{J}}\nu_j\boldsymbol{\Lambda}^{j+2}\bigg\} + \mathrm{Tr}\left\{\boldsymbol{\Lambda}\right\} + \mathrm{Tr}\bigg\{\boldsymbol{\Lambda}\bigg(\sum_{i=0}^{\mathcal{J}}\nu_j\boldsymbol{\Lambda}^{j+1}\bigg)^2\bigg\}\Bigg] \end{aligned} \tag{B.30}$$

Defining Vandermode matrix $\mathbf{C}_2 \in \mathbb{R}^{K\times(\mathcal{J}+1)}$, where $[\mathbf{C}_2]_{i,j} = \lambda_i^{j-1}$, we can rewrite (B.30) in compact form as $P_{\mathrm{AN}} =$

$$qN_T\mathrm{Tr}\left\{\mathbf{D}_{nn}\right\}\lim_{K\to\infty}\frac{1}{K}\mathbb{E}\Big[-2\boldsymbol{\nu}^T\mathbf{C}_2^T\boldsymbol{\Lambda}\boldsymbol{\lambda}+\mathbf{1}^T\boldsymbol{\lambda}+\boldsymbol{\nu}^T\mathbf{C}_2^T\boldsymbol{\Lambda}^3\mathbf{C}_2\boldsymbol{\nu}\Big]+(1-\phi)P_T\mathrm{Tr}\{\mathbf{D}_{nn}\boldsymbol{\Delta}_n\}, \tag{B.31}$$

where $\mathbf{1}$ denotes the all-ones column vector. Taking into account the constraint in (3.33), we can formulate the Lagrangian as

$$\mathcal{L}_2(\boldsymbol{\nu}) = P_{\mathrm{AN}} + \epsilon_2(\lim_{K\to\infty}\frac{1}{K}\mathbb{E}[\boldsymbol{\nu}^T\mathbf{C}_2^T\boldsymbol{\Lambda}^2\mathbf{C}_2\boldsymbol{\nu} - 2\boldsymbol{\nu}^T\mathbf{C}_2^T\boldsymbol{\lambda}] + 1) \tag{B.32}$$

with Lagrangian multiplier ϵ_2. The optimal coefficient vector $\boldsymbol{\nu}_{\mathrm{opt}}$ is then obtained by taking the gradient of the Lagrangian function with respect to $\boldsymbol{\nu}$ and setting it to zero:

$$\lim_{K\to\infty} \mathbb{E}\left[\mathbf{C}_2^T \boldsymbol{\Lambda}^2 \left(\boldsymbol{\Lambda} + \epsilon \mathbf{I}_K\right) \mathbf{C}_2\right] \boldsymbol{\nu} = \lim_{K\to\infty} \mathbb{E}\left[\mathbf{C}_2^T \left(\boldsymbol{\Lambda} + \epsilon \mathbf{I}_K\right) \boldsymbol{\lambda}\right], \tag{B.33}$$

where we used $\epsilon = \frac{\epsilon_2}{qN_T \mathrm{Tr}\{\mathbf{D}_{nn}\}}$. Simplifying the terms in (B.33) by exploiting a similar approach as in Appendix B.5, we obtain the result in Theorem 3.2.

Appendix C

Proofs in Chapter 4

Appendix C provides the proofs of Lemmas in Chapter 4.

C.1 Proof of Lemma 4.1

The ergodic secrecy rate achieved by the k^{th} MT in symbol interval $t \in \{B+1, \ldots, T\}$ is given by [43, Lemma 1]

$$R_k^{\text{sec}}(t) = \mathbb{E}\left[[R_k(t) - \log_2(1+\gamma_E)]^+\right] \geq [\mathbb{E}[R_k(t)] - C_E]^+ \overset{(a)}{\geq} [\underline{R}_k(t) - C_E]^+ = \underline{R}_k^{\text{sec}}(t), \tag{C.1}$$

where $\underline{R}_k^{\text{sec}}(t)$ is an achievable lower bound for $R_k^{\text{sec}}(t)$, and (a) uses (4.17). By averaging $R_k^{\text{sec}}(t)$ over all symbol intervals $t \in \{B+1, \ldots, T\}$ we obtain Lemma 4.1. This completes the proof.

C.2 Proof of Lemma 4.2

The expectation given in (4.20) for $k \in \mathcal{S}_b$ is calculated as

$$\begin{aligned}
\mathbb{E}\left[\mathbf{g}_k^H \boldsymbol{\Theta}_k^H(t)\mathbf{f}_k\right] &\overset{(a)}{=} \mathbb{E}\left[\frac{\hat{\mathbf{g}}_k^H \boldsymbol{\Psi}_{t_0}^H(t)\hat{\mathbf{g}}_k}{\|\hat{\mathbf{g}}_k\|} e^{j(\phi_k(t)-\phi_k(t_0))}\right] \\
&\overset{(b)}{=} \operatorname{tr}\left(\mathbb{E}\left[\frac{\hat{\mathbf{g}}_k\hat{\mathbf{g}}_k^H}{\|\hat{\mathbf{g}}_k\|}\right]\mathbb{E}\left[\boldsymbol{\Psi}_{t_0}^H(t)\right]\right)\mathbb{E}\left[e^{j(\phi_k(t)-\phi_k(t_0))}\right] \\
&= \sqrt{\beta_k N \lambda_k} \cdot e^{-\frac{\sigma_\psi^2+\sigma_\phi^2}{2}|t-t_0|},
\end{aligned} \tag{C.2}$$

where $\mathbf{\Psi}_{t_0}(t) = \mathrm{diag}\left(e^{j(\psi_1(t)-\psi_1(t_0))}\mathbf{1}^T_{1\times N/N_o}, \ldots, e^{j(\psi_{N_o}(t)-\psi_{N_o}(t_0))}\mathbf{1}^T_{1\times N/N_o}\right)$ and λ_k is defined in Lemma 4.2. In (C.2), (a) exploits that the channel estimate and the estimation error are uncorrelated [18], and (b) exploits the mutually independence of $\hat{\mathbf{g}}_k\hat{\mathbf{g}}_k^H$, $\mathbf{\Psi}^H_{t_0}(t)$, and $e^{j(\phi_k(t)-\phi_k(t_0))}$. This completes the proof.

C.3 Proof of Lemma 4.3

In (4.18), the term reflecting the interference caused by the signal intended for MT $l \in \mathcal{S}_b$ to MT $k \in \mathcal{S}_b$ can be expanded as

$$\begin{aligned}
\mathbb{E}\left[\left|\mathbf{g}_k^H\mathbf{\Theta}_k^H(t)\mathbf{f}_l\right|^2\right] &= \mathbb{E}\left[\left|\mathbf{g}_k^H(t_0)\mathbf{\Psi}^H_{t_0}(t)\frac{\hat{\mathbf{g}}_l}{\|\hat{\mathbf{g}}_l\|}e^{j(\phi_k(t)-\phi_k(t_0))}\right|^2\right] \\
&= \mathbb{E}\left[\mathrm{tr}\left(\mathbf{g}_k(t_0)\mathbf{g}_k^H(t_0)\mathbf{\Psi}^H_{t_0}(t)\frac{\hat{\mathbf{g}}_l\hat{\mathbf{g}}_l^H}{\|\hat{\mathbf{g}}_l\|^2}\mathbf{\Psi}_{t_0}(t)\right)\right] \\
&\overset{(a)}{=} \beta_k + \left(\frac{I}{\beta_l^2\boldsymbol{\omega}_l^H\mathbf{\Theta}^b_{\sigma(t_0)}\mathbf{\Sigma}_b^{-1}\mathbf{\Theta}^H_{\sigma(t_0)}\boldsymbol{\omega}_l N} - \beta_k\right) \\
&\times\ \mathbb{E}_\psi\left[\left(\frac{1}{N}\mathrm{tr}\left(\mathbf{\Psi}^H_{t_0}(t)\right)\right)^2\right],
\end{aligned} \tag{C.3}$$

where $\mathbf{X}_l = \beta_l\boldsymbol{\omega}_l^H\mathbf{\Theta}^b_{\sigma(t_0)}\mathbf{\Sigma}_b^{-1}\otimes\mathbf{I}_N$ and $I = \mathbb{E}\left[\mathrm{tr}\left(\mathbf{X}_l^H\mathbf{g}_k(t_0)\mathbf{g}_k^H(t_0)\mathbf{X}_l\boldsymbol{\psi}_b\boldsymbol{\psi}_b^H\right)\right]$. (a) exploits [66, Theorem 1] from free probability theory, since the phase drift matrices $\mathbf{\Psi}_{t_0}(t)$ and $\mathbf{\Psi}^H_{t_0}(t)$ are free from $\mathbf{g}_k(t_0)\mathbf{g}_k^H(t_0)$ and $\frac{\hat{\mathbf{g}}_l\hat{\mathbf{g}}_l^H}{\|\hat{\mathbf{g}}_l\|^2}$. The further step is to expand I as

$$\begin{aligned}
I &= \mathbb{E}\left[\mathrm{tr}\left(\mathbf{Y}_{lk}^H\mathbf{g}_k\mathbf{g}_k^H\mathbf{Y}_{lk}\mathbf{g}_k\mathbf{g}_k^H\right)\right] + \mathrm{tr}\left(\beta_k\mathbf{X}_l^H\mathbf{X}_l(\mathbf{\Sigma}_b - \beta_k\left(\mathbf{W}_k^b + \mathbf{U}_k^b\right))\otimes\mathbf{I}_N\right) + \\
&\quad \mathbb{E}\left[\mathrm{tr}\left(\mathbf{X}_l^H\mathbf{g}_k\mathbf{g}_k^H\mathbf{X}_l\left(\mathbf{U}_k^b\otimes\mathrm{diag}\left(g_k^{(1)},\ldots,g_k^{(N)}\right)\right)\right)\right],
\end{aligned} \tag{C.4}$$

where

$$\mathbf{Y}_{lk} = \boldsymbol{\Theta}_k^H(t_0)\mathbf{X}_l \left[\boldsymbol{\Theta}_k^H(\overline{B}_{b-1}+1)\omega_k(\overline{B}_{b-1}+1), \ldots, \boldsymbol{\Theta}_k^H(t_0)\omega_k(t_0)\right]^T. \tag{C.5}$$

Denoting the t^{th} column of $\mathbf{I}_N$ by $\mathbf{e}_t^N \in \mathbb{C}^{N\times 1}$, the first term on the right hand side of (C.4), denoted by I_1, can be expanded as

$$\begin{aligned} I_1 &= \sum_{n_1,n_2,b_1,b_2} [\beta_k \mathbf{X}_l \mathbf{e}_{b_1}^{B_b} \otimes \mathbf{I}_N]_{n_1 n_1} [\beta_k \mathbf{X}_l \mathbf{e}_{b_2}^{B_b} \otimes \mathbf{I}_N]_{n_2 n_2}^H \times \omega_k(b_1)\omega_k^*(b_2)\Theta(n_1,n_2,b_1,b_2,t_0) \\ &= \left|\text{tr}\left(\beta_k \mathbf{X}_l (\boldsymbol{\Theta}_{\sigma(t_0)}^b \boldsymbol{\omega}_k \otimes \mathbf{I}_N)\right)\right|^2 + \text{tr}\left(\beta_k^2 \mathbf{X}_l^H \mathbf{X}_l (\mathbf{W}_k^b \otimes \mathbf{I}_N)\right) \\ &+ \sum_{|n_1-n_2|\leq \frac{N}{N_0}}^{N} \beta_k^2 (\mathbf{e}_{n_1}^N)^H \mathbf{X}_l \left((\mathbf{W}_k^b - \boldsymbol{\Theta}_{\sigma(t_0)}^b \boldsymbol{\omega}_k \boldsymbol{\omega}_k^H \boldsymbol{\Theta}_{\sigma(t_0)}^b) \otimes \mathbf{e}_{n_1}^N (\mathbf{e}_{n_2}^N)^H\right) \mathbf{X}_l^H \mathbf{e}_{n_2}^N, \end{aligned} \tag{C.6}$$

where the expectation with respect to the phase drift, $\Theta(n_1,n_2,b_1,b_2,t_0)$, depends on the number of LOs, N_o, and is given by $\Theta(n_1,n_2,b_1,b_2,t_0) =$

$$\mathbb{E}\left[e^{\theta_k^{n_1}(b_1)-\theta_k^{n_1}(t_0)-\theta_k^{n_2}(b_2)+\theta_k^{n_2}(t_0)}\right] = \begin{cases} e^{-\frac{\sigma_\psi^2+\sigma_\phi^2}{2}|b_1-b_2|} & |n_1-n_2| \leq \frac{N}{N_o}, \\ e^{-\frac{\sigma_\psi^2+\sigma_\phi^2}{2}|t_0-b_1|} e^{-\frac{\sigma_\psi^2+\sigma_\phi^2}{2}|t_0-b_2|} & |n_1-n_2| > \frac{N}{N_o}. \end{cases} \tag{C.7}$$

Furthermore, we rewrite $\mathbf{U}_k^b = (\kappa_t^{\text{MT}}+\kappa_r^{\text{BS}})p_\tau \sum_{t=1}^{B_b} \mathbf{e}_t^{B_b}(\mathbf{e}_t^{B_b})^H$ and $\text{diag}\left(g_k^{(1)}, \ldots, g_k^{(N)}\right) = \sum_{n=1}^N |(\mathbf{e}_n^N)^H \mathbf{g}_k|^2 \mathbf{e}_n^N (\mathbf{e}_n^N)^H$. Using these results in the third term on the right hand side of (C.4), denoted by I_2, we obtain

$$I_2 = \beta_k^2 \text{tr}\left(\mathbf{X}_l^H \mathbf{X}_l (\mathbf{U}_k^b \otimes \mathbf{I}_N)\right) + \sum_{n=1}^N \beta_k^2 (\mathbf{e}_n^N)^H \mathbf{X}_l \left(\mathbf{U}_k^b \otimes \mathbf{e}_n^N (\mathbf{e}_n^N)^H\right) \mathbf{X}_l \mathbf{e}_n^N. \tag{C.8}$$

Applying (C.6) and (C.8) in (C.3) and exploiting $\mathbb{E}\left[\left(\frac{1}{N}\text{tr}\left(\boldsymbol{\Psi}_{t_0}^H(t)\right)\right)^2\right] = \frac{1-\epsilon}{N_o} + \epsilon$, we obtain the result in Lemma 4.3 for $k, l \in \mathcal{S}_b$.

For the case of $l \notin \mathcal{S}_b$, the multiuser interference term simplifies to

$$\mathbb{E}\left[\left|\mathbf{g}_k^H \boldsymbol{\Theta}_k^H(t)\mathbf{f}_l\right|^2\right] = \mathbb{E}\left[\left|\mathbf{g}_k^H(t_0)\boldsymbol{\Psi}_{t_0}^H(t)\frac{\hat{\mathbf{g}}_l}{\|\hat{\mathbf{g}}_l\|}e^{j(\phi_k(t)-\phi_k(t_0))}\right|^2\right] = \beta_k, \tag{C.9}$$

where the last equality follows from the independence of $\mathbf{g}_k$, $\hat{\mathbf{g}}_l$, $l \notin \mathcal{S}_b$, and $\boldsymbol{\Psi}_{t_0}^H(t)$. This completes the proof.

C.4 Proof of Lemma 4.4

The AN leakage power received at the k^{th} MT in time slot t can be expanded as

$$L_{\text{AN}}^k(t) = \mathbb{E}\left[\text{tr}\left(\hat{\mathbf{g}}_k\hat{\mathbf{g}}_k^H\boldsymbol{\Psi}_{t_0}^H(t)\mathbf{A}\mathbf{A}^H\boldsymbol{\Psi}_{t_0}(t)\right)\right] + \mathbb{E}\left[\mathbf{e}_k^H(t_0)\boldsymbol{\Psi}_{t_0}^H(t)\mathbf{A}\mathbf{A}^H\boldsymbol{\Psi}_{t_0}^H(t)\mathbf{e}_k(t_0)\right]. \tag{C.10}$$

By using [66, Theorem 1], the first term in (C.10) can be further expanded as

$$\beta_k L + \left(\mathbb{E}\left[\text{tr}\left(\hat{\mathbf{g}}_k\hat{\mathbf{g}}_k^H\mathbf{A}\mathbf{A}^H\right)\right] - \beta_k L\right)\mathbb{E}_\psi\left[\left(\frac{1}{N}\text{tr}\left(\boldsymbol{\Psi}_{t_0}(t)\right)\right)^2\right] = \beta_k L\left(1-\frac{1}{N_o}\right)(1-\epsilon), \tag{C.11}$$

since phase drift matrices $\boldsymbol{\Psi}_{t_0}(t)$ and $\boldsymbol{\Psi}_{t_0}^H(t)$ are free from $\hat{\mathbf{g}}_k\hat{\mathbf{g}}_k^H$ and $\mathbf{A}\mathbf{A}^H$. Furthermore, we exploited $\hat{\mathbf{g}}_k^H\mathbf{A} = \mathbf{0}$, $1 \le k \le K$, which holds for the NS AN precoder.

The second term in (C.10) is equal to $\beta_k L(1-\lambda_k)$, with λ_k as defined in Lemma 4.2, due to the mutual independence of the estimation error vector $\mathbf{e}_k(t_0)$, the phase drift matrix $\boldsymbol{\Psi}_{t_0}(t)$, and the AN precoder $\mathbf{A}$. Combining these two terms completes the proof.

C.5 Proof of Lemma 4.5

For the G-NS AN precoder, we rewrite the leakage power received at the k^{th} MT in time slot t as

$$L_{\text{AN}}^{k} = \sum_{m=1}^{M_o} \mathbb{E}\left[\left(\mathbf{g}_k^{(m)}\right)^H \left(\boldsymbol{\Theta}_k^{(m)}(t)\right)^H \mathbf{A}_{(m)} \mathbf{A}_{(m)}^H \boldsymbol{\Theta}_k^{(m)}(t) \mathbf{g}_k^{(m)} \right], \tag{C.12}$$

where $\mathbf{g}_k^{(m)} \in \mathbb{C}^{N/M_o \times 1}$ contains the $((m-1)N/M_o+1)^{\text{th}}$ to the $(mN/M_o)^{\text{th}}$ elements of vector $\mathbf{g}_k$, $1 \leq m \leq M_o$, and $\boldsymbol{\Theta}_k^{(m)}(t) \in \mathbb{C}^{N/M_o \times N/M_o}$ is a diagonal matrix with the $((m-1)N/M_o+1)^{\text{th}}$ to the $(mN/M_o)^{\text{th}}$ elements of matrix $\boldsymbol{\Theta}_k(t)$ on its main diagonal. Using similar steps as in Appendix C.4 but with N_o/M_o substituted by N_o for calculation of the expectation terms in (C.12), we obtain (4.30). This completes the proof.