Impact of Hardware Impairments on the Physical Layer Security of Cell-Free Massive MIMO

Ayesha Tahreem

Supervisor: Prof. Salama Ikki

Dr. Deeb Tubail

Department of Electrical Engineering

Lakehead University

A Thesis Presented to Lakehead University in Partial Fulfillment of the Requirement for the Degree of Master of Science in Electrical and Computer Engineering

May 2024

I would like to dedicate this thesis to my parents

Muhammad Hafeez & Faiza Hafeez. . .

Declaration

I hereby confirm that the entirety of the work contained therein is my own, original work, that I am the owner of the copyright thereof (unless to the extent explicitly otherwise stated). I understand that my thesis may be made electronically available to the public.

Ayesha Tahreem

May 2024

Examinary Committee

The following served on the Examining Committee for this thesis:

Supervisor

Dr. Salama Ikki, Professor, Department of Electrical and Computer Engineering.

Co-supervisor

Dr. Deeb Tubail, Department of Electrical and Computer Engineering.

Committee Members

Dr. Waleed Ejaz, Associate Professor, Department of Electrical and Computer Engineering.

Dr. Shafiqul Hai, Assistant Professor, Department of Electrical and Computer Engineering.

Session Chair

Dr. Ehsan Atoofian, Assistant Professor, Department of Electrical and Computer Engineering.

Acknowledgements

First and foremost, I am deeply grateful to almighty Allah for giving me the privilege of accomplishing this degree. I extend my sincere appreciation to my co-supervisor, Dr. Deeb Tubail for his invaluable guidance and unwavering support throughout my thesis and master's journey. His assistance and meticulous proofreading of my thesis have been instrumental in shaping its quality. Thank you for your dedication and expertise.

A special acknowledgment goes to my supervisor, Prof. Salama Ikki who has not only supported me and guided me, but also inspired me with his passion for research excellence. I am privileged to have such an exceptional supervisor. I am also grateful to the members of my thesis committee, Dr. Waleed Ejaz, Dr. Shafiqul Hai and Dr. Ehsan Atoofian for their valuable feedback and suggestions.

I am incredibly thankful to my mother who motivated me to acquire this degree and pushes me to be the best version of myself everyday. I am also very grateful to my father who has been there for me every step of the way. Their love and guidance is the reason behind my success. I would like to acknowledge my brother Abubakar for making my days brighter. I would also like to acknowledge my friends Samra, Sabyah and Maryum who truly inspire me and motivate me to pursue my goals eveyday.

Abstract

The development of new technologies and applications such as virtual reality, ultra-high-definition video conferencing, and Internet of Things (IoT) has caused a substantial increase in the demand for higher data rate in cellular systems. Massive Multiple-Input Multiple-Output (MaMIMO) is a reliable solution to fulfill this demand, not only providing higher data rates, but also offering enhanced coverage and network capacity. These aspects are essential to accommodate the rapidly increasing number of mobile subscribers with each passing year. However, the swift progression of wireless communication technologies, including fifth-generation (5G) networks and beyond raises a critical concern: ensuring the security of these systems.

This thesis focuses on enhancing the security of Cell-Free Massive Multiple-Input Multiple-Output (CF-MaMIMO), an advanced extension of MaMIMO. It uses a Physical Layer Security (PLS) technique which involves beamforming artificial noise (AN) in the null of the users. Previous studies have demonstrated that implementing PLS techniques always enhance the security performance of wireless communication systems. However, these studies often overlook a crucial aspect: the impact of hardware impairments (HWIs). They assume ideal transceivers in their research, neglecting the practical implications where hardware non-idealities can significantly impact system security. Therefore, this thesis analyzes the impact of HWIs on security performance based on broadcasting AN as a PLS technique in CF-MaMIMO systems. For this purpose, the Signal-to-interference-plus-noise ratio (SINR) of the legitimate users and Signal-to-noise ratio (SNR) of the eavesdroppers is derived considering HWIs in the implementation of AN broadcasting. Contrary to existing literature, it is demonstrated in this thesis that in certain instances, the AN leads to

degradation in the security performance of the system due to HWIs. The findings of this study reveal that fluctuations in the hardware quality of users, eavesdroppers and access points (APs) directly affect the system's security. Furthermore, these findings emphasize the significance of considering hardware quality when applying PLS techniques by broadcasting AN to maximize security performance.

Table of contents

List of figures

List of tables

Nomenclature

Subscripts

$\mathbf{A}$	Matrix
$\mathbf{a}$	Column vector
a	Scalar
$[\mathbf{A}]_{ij}$	The element of a matrix $\mathbf{A}$ in the i^{th} row and the j^{th} column
$CN(\mu, \sigma^2)$	Complex Gaussian random variable with mean μ and variance σ^2
$\mathbb{E}\{\cdot\}$	Statistical expectation
$(\cdot)^{\text{H}}$	Hermitian operator
$\mathbf{I}_M$	Identity matrix of size M
$(\cdot)^{\text{T}}$	Transpose operator
$\text{tr}[\mathbf{A}]$	Trace of a square matrix $\mathbf{A}$

Acronyms / Abbreviations

5G	Fifth-Generation
AN	Artificial Noise
AP	Access Point

AWGN Additive White Gaussian Noise

BS Base Station

CF-MaMIMO Cell-Free Massive Multiple-Input Multiple-Output

COMAR Committee on Man and Radiation

CSI Channel State Information

HWI Hardware Impairment

I In-phase

IoT Internet of Things

MaMIMO Massive Multiple-Input Multiple-Output

MIMO Multiple-Input Multiple-Output

NLoS Non-Line-of-Sight

PLS Physical Layer Security

Q Quadrature

SE Spectral Efficiency

SINR Signal-to-Interference-plus-Noise Ratio

SISO Single-Input Single-Output

SNR Signal-to-Noise Ratio

ER Eavesdropper Rate

SSR Secrecy Sum Rate

USR User Sum Rate

ZF Zero-forcing

Chapter 1

Introduction

This chapter presents a comprehensive overview of the focus areas investigated in this thesis. It commences with exploring the current landscape in wireless communications, emphasizing available security methods. The subsequent section outlines the key concepts of MaMIMO systems, including background on CF-MaMIMO, security challenges and corresponding solutions, as well as environmental and safety aspects. Moreover, the chapter offers an overview of transceiver HWIs. Finally, it concludes with a summary of the objectives, the contributions of the thesis, and the organizational structure for the remainder of the thesis.

1.1 Securing Wireless Communication Networks

1.1.1 Navigating Cyber Threats in Wireless Communication

In today's world, wireless communication technology is essential to human life as it facilitates data transmission. Often, this data contains private information such as government-classified information, financial records, and multimedia. According to the International Telecommunication Union, approximately 67 percent of the world's population, amounting to 5.4 billion people globally, used the internet in 2023 [1]. As wireless networks expand and new applications emerge, there is an upcoming surge in mobile subscribers. Thus, this number is expected to rise. However, there is a growing trend of mobile and wireless devices being

targeted by cybercriminal activities. A leading cybersecurity research firm, Cyber Security Ventures, predicts that the annual global cost of cybercrime will increase from 3 trillion dollars in 2015 to 10.5 trillion in 2025 [2]. That is more than triple the amount in just a decade, emphasizing the urgent need to enhance the protection of wireless communication networks against cybercriminal activities.

Traditionally, the upper layers of the open system interconnect model resolve discrepancies in data transmission characteristics, including authenticity, confidentiality, and privacy. These attributes depend on cryptographic algorithms such as public-key encryption, symmetric encryption, and key distribution, which operate independently of the physical layer [3]. Given eavesdroppers' limited computing power, these techniques are suitable security measures. However, they rely on computational complexity for robustness. Yet, with the current advancements in quantum computing, existing cryptographic algorithms face risks due to the limitless computational capacity of quantum systems [4]. This indicates that conventional cryptographic algorithms used to secure wireless communication have limitations in terms of reliability.

With wireless networks' inherent openness and superposition characteristics, there arises a concern regarding the confidentiality and security of transmitted information in the presence of unauthorized parties. These attacks pose a key challenge for system designers in constructing next-generation wireless networks [5], [6]. The inherent broadcast properties of the system disrupt data transmission from reaching unintended users. Conversely, variations in time within the wireless channel lead to the reception of multiple copies of the transmitted signal at the receiver end.

Eavesdropping attacks in wireless networks are classified as passive or active attacks [7], [8]. In passive attacks, eavesdroppers silently listen to ongoing transmissions, attempting to steal transmitted data without interfering with legitimate communication. On the other hand, active eavesdropper attacks employ more intrusive and aggressive strategies, attempting to degrade signal quality at the intended receiver. These strategies include denial of service, routing, and node malfunction attacks [7]. Given the wide variety of security threats, wireless networks must possess specific capabilities to resist and mitigate these challenges. To ensure

network security, integrity, confidentiality, authentication, availability, and access control should all be considered [7].

1.1.2 A Comparative Perspective: Cryptography vs. PLS in Wireless Communication

In most instances, cryptography is the primary technology to address security concerns in traditional and contemporary electronic communication systems. From an alternative viewpoint, certain innovative technologies, especially quantum computing, pose a threat to systems that rely on cryptographic security algorithms [8]. Quantum computers possess almost limitless computing capabilities, enabling them to break encryption and decryption keys easily. They break the keys by predicting secret keys or rapidly performing reverse calculations, allowing unauthorized or masked users to access and tap the ongoing data transmission [4]. However, quantum computing is limited in breaking all types of cryptographic algorithms, meaning that it is only harmful to specific systems based on cryptography. Additionally, cryptographic procedures can introduce delays, which may be undesirable in certain applications, such as 5G ultra-reliable low-latency communication [9]. Furthermore, the processes in cryptography necessitate extra resources for computations, resulting in low energy consumption efficiency. Therefore, there is a need to introduce new security measures to further enhance the system's security in addition to cryptographic methods. One of these techniques to counteract the limitations of cryptographic algorithms is PLS.

PLS differs from cryptographic technology because it is based on the concept of information-theoretic security proposed by Wyner [10]. In the PLS technique, communication between two legitimate users in the presence of an unauthorized user is represented as a discrete memory-less wiretap channel [11]. Compared to cryptographic algorithms, PLS techniques prevent unauthorized users from tapping the data. PLS does not require encryption in the upper layers to secure the network; rather, it exploits wireless channel characteristics through signalling and channel coding [12]. A key characteristic of PLS techniques is their proven

ability to effectively secure the system even with the near-limitless computational resources of the network intruders.

Although PLS offers extensive benefits, it has certain limitations worth considering. As evident in [13], PLS is not able to accomplish absolute security due to its reliance on average information. Furthermore, most PLS techniques assume that prior knowledge of the eavesdropper's wiretap channel is available; however, in practical applications, this information is not possible to acquire [8]. Moreover, using PLS schemes as the sole security measure will be difficult to implement in future wireless networks as it requires a high data rate to secure the system. Therefore, PLS can be coupled with additional upper-layer security schemes to ensure the robustness and protection of wireless communication networks.

1.2 Overview of MaMIMO

1.2.1 The Origination of MaMIMO

Before the widespread adoption of MIMO, single-input-single-output (SISO) systems were predominantly used. The main drawbacks of SISO systems include very low throughput and the inability to accommodate many users with high reliability [14]. For wireless communication systems to support more users, various new MIMO technologies have been established, however, not enough to fulfill the ever-growing demands [14]. The number of wireless users has increased exponentially over the last couple of years, producing a massive amount of data that requires efficient and reliable handling [15]. As a matter of fact, a study by Ericsson Mobility predicts a surge in mobile network traffic by 77 percent, reaching 226 exabytes per month globally by 2026 [15].

Furthermore, wireless communication has undergone a transformative shift with the emergence of advanced technologies such as 5G networks, Machine-to-Machine communication, and the IoT. Moreover, billions of IoT devices support a wide variety of cutting-edge applications for smart homes, smart energy, smart healthcare, all of which contribute to the data traffic. It is predicted that there will be approximately 207 billion connected devices by the end of 2024 [16]. The central challenge is how wireless communications technologies can

fulfill this escalating need for connectivity. The solution lies in a powerful communication technology known as MaMIMO.

1.2.2 Advantages of MaMIMO

MaMIMO technology has emerged as a leading competitor in the realm of 5G networks, addressing the challenge posed by the vast amounts of data traffic [17]. Representing an advancement of modern MIMO systems, MaMIMO employs hundreds to thousands of antennas at the base station (BS), serving tens of users simultaneously [18], [19]. As more antennas are deployed in a MaMIMO system, the radiated beams from the BS become narrower, enabling the focus of these beams to be directed toward the desired user. Furthermore, these spatially focused beams enhance the throughput for the intended user while mitigating interference to neighboring users [20]. This capability allows MaMIMO to provide higher spectral efficiency (SE), achieving more than ten times better SE than conventional MIMO systems. It also enhances energy efficiency since the antenna array is focused in a specific direction, requiring less radiated power. Other notable advantages of MaMIMO include higher data rates and capacity resulting from the array gain and spatial multiplexing capabilities. Additionally, user tracking becomes more accurate and reliable due to MaMIMO's ability to use narrow signal beams directed toward the user. In addition, due to the orthogonal mobile station channel and narrow beams, MaMIMO offers enhanced PLS [21].

Another advantage of MaMIMO is its low power consumption since it is constructed with ultra-low power linear amplifiers, eliminating bulky electronic hardware in the communication system. Additionally, MaMIMO is resilient against fading effects attributed to the large number of antennas it employs [22]. The robustness of MaMIMO is demonstrated through its numerous benefits, where a particularly attractive feature of MaMIMO is its ability to operate despite the failure of one or a few antennas due to its vast quantity of antennas. Another benefit of the large number of antennas deployed by MaMIMO is more diversity gain, which improves the link reliability [20], [23]. Moreover, MaMIMO lowers air interference latency [24].

1.2.3 Practical Considerations

Despite the extensive benefits of wireless access technologies, they pose considerable environmental threats. MaMIMO stands out for its ability to minimize environmental impact. Since MaMIMO utilizes beamforming, it reduces environmental stray radiation. This is because it radiates energy in a particular direction as opposed to all directions [15]. Additionally, MaMIMO arrays enhance connectivity while consuming less power compared to alternative wireless technologies [15]. A study examining the characteristics of a 256 antenna array demonstrated that the MaMIMO BS delivers two hundred times the capacity of a 4G network for equivalent coverage while consuming one-eighth of the power [25], [15]. Similar energy-efficient models employing MaMIMO have been discovered by other researchers. In instances of low-traffic loads, some components of the antenna array can be deactivated, enabling lower power consumption and improving efficiency [15].

MaMIMO has proven to be safer for humans than other wireless communication technologies. This is attributed to the nature of beamforming technology, which ensures that only the desired user receives the signal [15]. Compared to conventional wireless systems that radiate signals throughout the cell, MaMIMO spatially focuses its energy towards the desired network users. Therefore, minimal collateral radiation affects individuals nearby [15]. Moreover, a group of experts that study health and safety issues associated with electromagnetic fields, known as the Committee on Man and Radiation (COMAR), determined that there are no inherent dangers of MaMIMO technology. Instead, any potential safety concern depends on the duration of exposure [15].

Overall, MaMIMO surpasses the conventional MIMO system with its extensive advantages, which are highlighted in Table 1.1.

Table 1.1 Comparison of Traditional MIMO and MaMIMO Systems

Parameter	**MIMO**	**MaMIMO**
Number of Antennas	≤ 8	≥ 16
Spectral Efficiency	Low	High
Throughput	Low	High
Noise Resistance	Low	High
Fading Resistance	Low	High
Diversity Gain	Low	High
Energy Efficiency	Low	High
Latency	High	Low
Cost	Low	High
Complexity	Low	High
Scalability	Low	High
Link Stability	Low	High

1.2.4 CF-MaMIMO

An evolving descendant of MaMIMO is the CF-MaMIMO technology, where a large number of service antennas, referred to as APs, serve a significantly smaller number of users distributed over a wide area. This approach allows the system to exploit diversity to mitigate the impact of shadow fading [26]. The distributed APs cooperate via a backhaul network, operating cohesively in phase. They serve all users in the same time-frequency resource [27]. Unlike conventional architectures, there are no cells or cell boundaries in the CF-MaMIMO system, which results in improved coverage and increased capacity. This cutting-edge wireless access technology is a key enabler for next-generation wireless systems. Fig. 1.1 compares the architecture of MaMIMO and CF-MaMIMO [28]. A summary of the CF-MaMIMO system is also provided in Table 1.2 [29]. The advantages and disadvantages of the CF-MaMIMO system are highlighted in Table 1.3 [29].

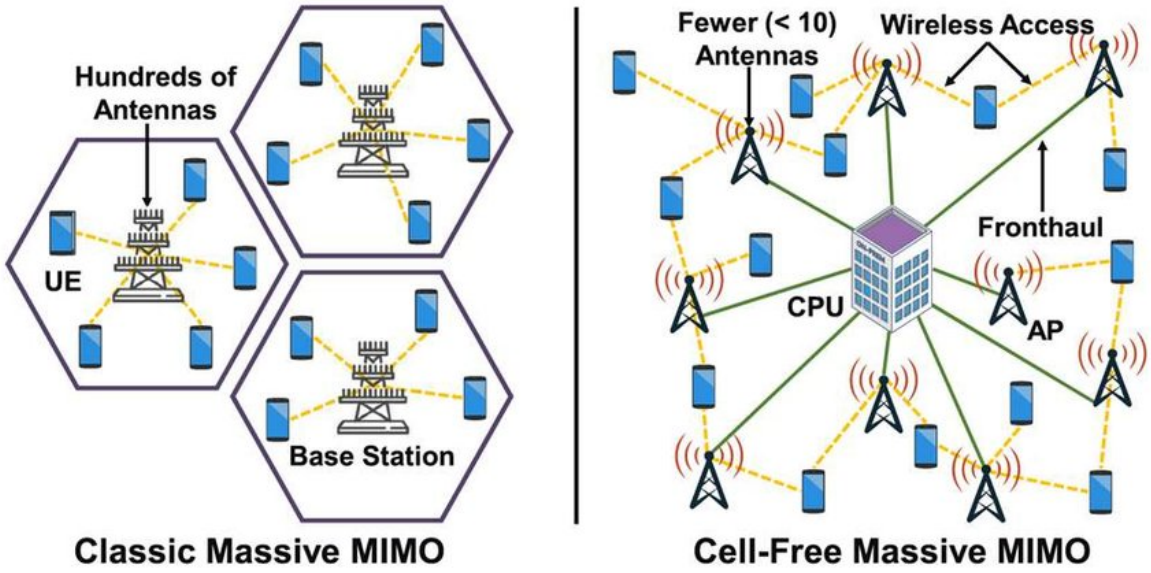

Fig. 1.1 MaMIMO vs CF-MaMIMO.

Table 1.2 Overview of CF-MaMIMO System

Feature	**Description**
Key Concepts	Massive number of APs distributed across a wide area
	Serve multiple users in the same time-frequency resource
Characteristics	Number of APs significantly greater than the number of users
	Spatially focused signals
Technical Content	Enhanced capacity and coverage
	High throughput
	High noise resistance
	High scalability
	High link stability

Table 1.3 Benefits and Challenges of CF-MaMIMO System

Category	Description
Benefits	High spectral efficiency
	Array gain
	High energy efficiency
	High data rate
	User tracking
	Low power consumption
	Less fading
	Low latency
	More reliability
Challenges	Pilot contamination
	Channel estimation
	Precoding
	User scheduling
	Hardware impairments
	Energy efficiency
	Signal detection

1.2.5 Security Challenges and Solutions

The focus of this thesis involves the application of PLS in CF-MaMIMO. The large number of antennas deployed in the CF-MaMIMO system creates a wider coverage area, which can attract unauthorized parties seeking to tap and access sensitive data transmitted over the wireless channel. The tapped data can be decoded, potentially compromising the secrecy of the communication. Addressing the security challenges associated with MaMIMO and CF-MaMIMO systems is crucial to ensure the confidentiality of the communication. This research uses PLS techniques, including beamforming and AN broadcasting, to secure the CF-MaMIMO system.

MaMIMO uses beamforming technology to direct the signal toward the intended user and nullify interference from other users. Beamforming utilizes phase shifting and amplitude control of the signal to steer the signal in a particular direction. The channel state information (CSI) is necessary to determine the optimal beamforming direction for each user, enabling simultaneous data transmission of multiple data streams. The key advantage of beamforming is its capability to maximize the SNR while preventing confidential information from reaching unintended users, especially eavesdroppers. This improves the system's energy efficiency since the energy is transmitted in a specific direction instead of diffusing out.

This study utilizes Zero-forcing (ZF) and Null Beamforming techniques. With ZF beamforming, data is transmitted directly to the users while simultaneously nullifying interference from other users in the network, as seen in Fig. 1.2. It involves aligning the transmitted signal with the desired channel response while ensuring orthogonality between the channel of users and those of other users within the system. ZF beamforming achieves this by adjusting the phase and amplitude of the transmitted signal for different antennas. This beamforming technique is beneficial for CF-MaMIMO systems in which multiple users are present. Additionally, AN is precisely transmitted in the null of the users using beamforming. The null of the users in this context refers to the region where the users are not located. It is determined by finding the mathematical null of the users' matrix. This technique improves the system's security by disrupting potential eavesdroppers attempting to intercept the information signal, as illustrated in Fig. 1.2. This security measure protects the system from potential eavesdroppers that lie in the null of the users. Null beamforming depends on the CSI of the users to precisely focus the AN toward the null space of their channels.

1.3 Transceiver Hardware Impairments

MaMIMO systems encompass a large amount of components, i.e. antennas, to mitigate the effects of noise, interference and fading. This massive number of antennas deployed in MaMIMO not only increases the complexity of the system but also the hardware costs.

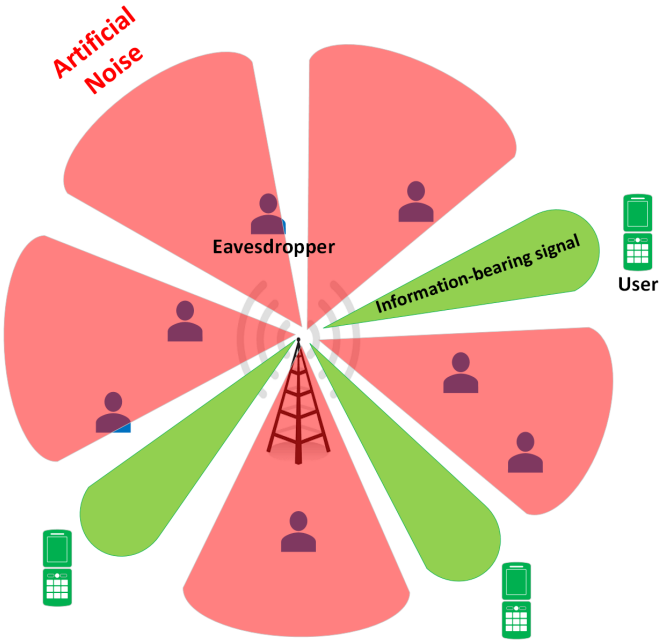

Fig. 1.2 Beamforming information-bearing signal to users and AN to the null of users.

Implementing MaMIMO requires small and low-cost components to lower the hardware size and computational complexity. However, low-cost components come with a cost-quality trade-off as these inexpensive components increase HWIs [30]. A MaMIMO BS with these HWIs is depicted in Fig. 1.3 [29]. The following are some of the hardware imperfections that are present in practical transceivers, which are mentioned in [31] and referenced therein:

- *Phase noise:*

  Oscillators play a crucial role in communication systems. The primary function of oscillators is to facilitate up-conversion and down-conversion. The performance of wireless communication systems is subjected to significant degradation when phase noise exists in the local oscillator. This degradation is especially evident when using low-cost hardware components for high-frequency operation. The phase noise in oscillators is generated by thermal noise in the oscillator circuit. Subsequently, the oscillator's phase experiences fluctuations, leading to potential errors in the transmission and reception of signals, which results in lower signal quality. The generation of phase noise at its core is attributed to the instabilities in oscillators, as well as minor

random deviations from the ideal frequency of the oscillator, resulting in a "jitter" in the signal's phase.

- *Non-linear power amplifiers:*

  The key purpose of power amplifiers is to amplify the signal power to an appropriate level to ensure effective transmission over the wireless channel. Furthermore, the power amplifier increases the input power signal by multiplying the input signal with a constant gain. This gain is selected so the amplifier does not enter the non-linear regions, resulting in distortion and interference due to out-of-bad emissions generation. Non-linearities in power amplifiers exist in the case of high-efficiency, near-saturation operation. These non-linearities subject the transmitted signal to amplitude and phase distortions, causing spectral regrowth. This regrowth may interfere with adjacent frequency bands. Moreover, power amplifier linearities in multi-carrier systems, such as orthogonal frequency division multiplexing, intensify inter-modulation distortion and inter-carrier interference, leading to deterioration of the system's bit error rate. Therefore, it is essential to consider the impact of power amplifier non-linearities and establish mitigation strategies to maximize system performance.

- *I/Q imbalance:*

  The in-phase (I) and quadrature (Q) branches are crucial in determining the received signal's quality in communication systems. However, in practice, the imperfect matching between the I and Q branches results in HWIs termed in-phase and quadrature imbalances. This imbalance arises from non-idealities in analog circuits, such as amplitude or phase differences of the I and Q signal components. Furthermore, I and Q imbalances decrease the signal quality and significantly reduce the system's performance.

With the massive amount of antennas deployed in MaMIMO, there is mutual coupling between the antenna elements, leading to significant changes in the load impedance, generating distortions [32]. Despite the remarkable ability of MaMIMO to reduce the radiated power 100 times less than that of traditional MIMO systems, the energy consumption of baseband

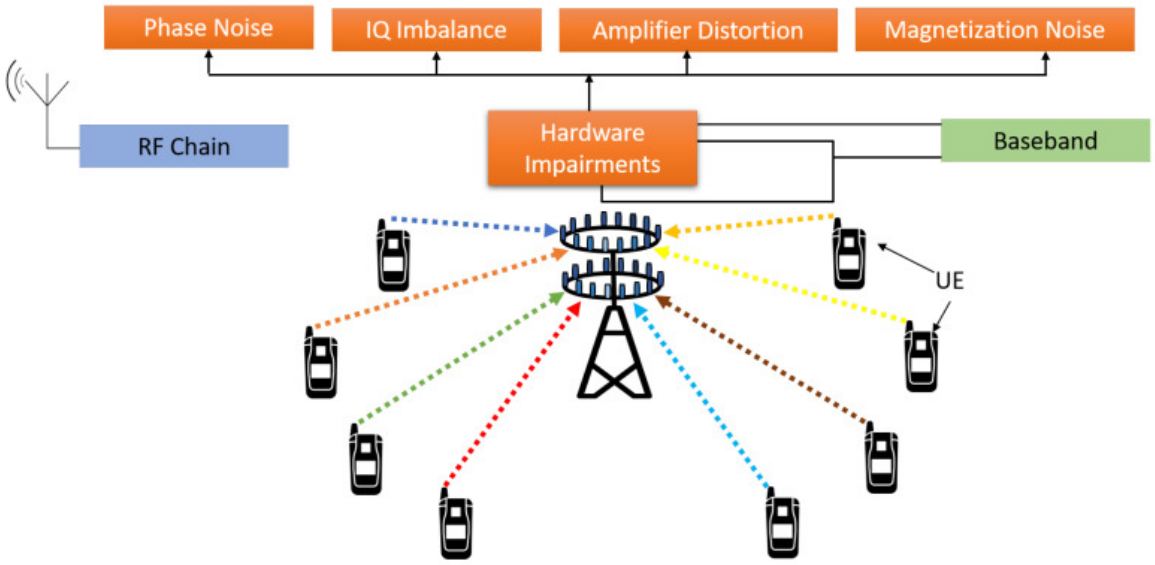

Fig. 1.3 MaMIMO BS with HWIs

hardware and data converters rises linearly with the addition of antennas. Furthermore, the primary drawback of using inexpensive phase-locked loops and oscillators is that it increases the phase shift between the arrival times of the pilot and data signals at each antenna. Consequently, this limitation constraints the performance of MaMIMO [17]. Fig. 1.3 represents a MaMIMO BS with HWIs.

Despite using algorithms to mitigate the influence of HWIs, residual HWIs remain. Phase noise estimation and compensation algorithms tackle issues associated with phase distortion, while digital pre-distortion algorithms compensate for power amplifier non-linearities. The use of these HWIs algorithms is not compatible with a large number of antennas since computation complexity increases exponentially [33], [34]. The phase shift issue can be minimized using smart transmission physical layer schemes. Base-band signal processing costs can be reduced by constructing dedicated hardware that can operate simultaneously. The effect of the inexpensive amplifier on the transmitter can be compensated by having a low Peak to Average Power Ratio (PAPR) [35].

1.4 Objectives

1. Past works in the area of MaMIMO systems [36], [37], [38], [39] lack the consideration of the detrimental effects of HWIs in the application of PLS techniques. This research addresses this issue by investigating the impact of HWIs on the security and performance of the CF-MaMIMO system. Specifically, we implement a PLS technique to protect the system from passive eavesdropping attacks. The PLS technique involves ZF beamforming of data streams to legitimate users and AN broadcasting to the null of those users. Furthermore, it evaluates and analyzes the effect of elevating AN power levels considering various hardware quality conditions including ideal and non-ideal. The assessment of system and security performance was performed through metrics including User Sum Rate (USR), Eavesdropper Rate (ER) and Secrecy Sum Rate (SSR).

2. The degradation of system performance due to HWIs can be compensated by recommending and applying strategies to enhance system performance. The first strategy is to increase the transmitted power and analyze the performance of the system under various hardware conditions of the communication systems' components. The second strategy is to increase the quantity of APs and analyze its effects on the security and performance of the system considering various hardware scenarios of the users, eavesdroppers and APs.

3. Identify and analyze practical implementation challenges related to deploying CF-MaMIMO systems with hardware imperfections and broadcasting AN. Describe the cost-quality trade-offs introduced by HWIs as well as issues arising from increasing the AN power as well as the transmitted power in real-world scenarios. Furthermore, assess the practical challenges of deploying additional APs in terms of energy efficiency and costs.

1.5 Contribution

In this study, an investigation is conducted to examine the influence of HWIs on the security performance of the CF-MaMIMO system under practical conditions. Previous studies in [40], [41] and [42] found that broadcasting AN always enhances the security performance in MaMIMO systems. However, this is under the assumption that the transceiver is ideal. In this study, the presence of hardware non-idealities of the transceiver was considered while broadcasting AN. It was demonstrated that PLS techniques can degrade the system and security performance in certain instances. The SNR of legitimate users and eavesdroppers was derived to perform this investigation, factoring in the influence of HWIs alongside AN transmission. Overall, this research emphasizes the significance of the detrimental effects of hardware imperfections on the security and performance of the system.

1.6 Overview of Thesis Structure

This report has been organized as follows:

- *Chapter 2:*

  This chapter reviews existing literature on PLS in MaMIMO/CF-MaMIMO. It discusses PLS techniques such as AN generation to enhance communication security against eavesdropping attacks. Additionally, it explores works related to PLS integration in MaMIMO systems considering HWIs.

- *Chapter 3:*

  This chapter entails the system setup and mathematical modelling of the CF-MaMIMO system, elaborating on channel coefficients, fading characteristics, and beamforming strategies. Following this, it discusses the impact of HWIs on communication systems, modeling these impairments and integrating them into the system while applying PLS techniques to secure the system.

- *Chapter 4:*

  This chapter presents the simulations and results of the study, focusing on the impact of

HWIs coupled with PLS. It explores how elevating AN levels affects system security and performance. Moreover, the chapter examines the effects of HWIs under various scenarios, such as incrementing transmit power and deploying more APs, providing insights into their impact on the system.

This chapter provides a thorough outline of the key areas addressed in this thesis. It begins with an analysis of the current security methods, comparing conventional cryptographic methods and PLS. The chapter then explores MaMIMO and CF-MaMIMO, including their advantages and disadvantages. Next, the chapter focuses on challenges that arise from HWIs in the transceiver, describing particular types of HWIs. It highlights the objectives of this research, encompassing the impact of HWIs on system security and performance, recommending strategies to enhance system performance, and examining practical considerations. Finally, the chapter summarizes the objectives and contributions of the thesis, and provides an overview of the thesis structure.

Chapter 2

Literature Review

This literature review critically examines existing research relating to MaMIMO systems, aiming to provide a comprehensive understanding of the current security methodologies and identify gaps for further investigation. Through a systematic review of works, we seek to synthesize key findings, theoretical frameworks, and methodologies employed in previous studies. By contextualizing our research, we aim to contribute valuable insights regarding the influence of HWIs on the security performance of CF-MaMIMO systems.

2.1 Background

MaMIMO is an advanced wireless access technology that plays a key role in enabling 5G and beyond networks. An extension of MIMO technology, MaMIMO involves using hundreds to thousands of antennas connected to a BS to enhance system energy efficiency and SE [43]. This technology offers numerous advantages, including improved coverage and throughput. Moreover, in cellular communication, the signal weakens as the user moves away from the BS and closer to the cells' edge. In contrast, MaMIMO spatially focuses the signal to the user, improving performance at the cell edge [44]. Additionally, MaMIMO serves multiple users simultaneously within the same time-frequency resources [45].

Surpassing the exceptional capabilities of MaMIMO, CF-MaMIMO is a revolutionary technology wherein users are served by a large number of APs over a wide coverage area,

achieving substantial capacity enhancements. Moreover, due to the close proximity between users and APs, CF-MaMIMO significantly improves link reliability, offering high coverage probability. The inherent diversity gains introduced by a multitude of distributed antennas further contribute to reducing fading and shadowing effects [46]. The CF-MaMIMO architecture minimizes interference in cellular networks [47]. Notably, CF-MaMIMO's ability to deliver higher data rates represents a transformative advancement in wireless communications.

Although high data rate communication systems are core to enabling next-generation technologies, they are particularly vulnerable to eavesdropping attacks, where unauthorized users maliciously attempt to intercept secret data intended for legitimate recipients [48]. One conventional method of securing communication systems is through cryptography. This technique involves converting data into an unreadable format, ensuring that only authorized users can decipher it. In essence, cryptography employs encryption and decryption to safeguard the system against unauthorized users from eavesdropping on confidential messages. However, this traditional security approach suffers from inefficiencies in computational complexity, resulting in excessive energy consumption during computation processes.

PLS, a complementary security method to cryptography, has gained considerable interest [49]. This technique exploits the imperfection and noisiness of the underlying quantum nature of the wireless communication channel, directly securing the communication system at the physical layer [49]. In contrast to traditional encryption technology, PLS provides the following features and benefits: Firstly, PLS achieves keyless security, implying that encryption and decryption operations are not required. Secondly, PLS utilizes the time-varying and random nature of wireless channels. Additionally, the security performance of wireless communications can be improved by employing signal processing techniques to design suitable beamforming or power allocation strategies from the transmitter's viewpoint.

2.2 Implementation of PLS in MaMIMO systems

PLS techniques were founded based on perfect secrecy and have sparked significant interest in the past decade [50]. Works [51]-[67] investigated the implementation of PLS in MaMIMO

systems. A notable work [51] delved into implementing PLS concepts in MaMIMO systems by investigating downlink communication with passive eavesdropping and applying maximum ratio transmission precoding. The research presented the SSR computations for this scenario. Another key work in this research area [52] thoroughly explored the impact of imperfect channels on PLS in a MaMIMO system. Moreover, the work considered channel estimation errors resulting from white noise and outdated CSI errors during periods of dynamic user activity. However, the authors of the study did not consider estimation errors due to non-orthogonal pilots arising from asynchronous pilot signals and user mobility.

Works in [53], [54] demonstrated the substantial degradation of the secrecy performance of the MaMIMO systems due to pilot contamination and active pilot attacks. The study in [55] analyzes the security of data transmission with a passive multi-antenna eavesdropper in multi-cell MaMIMO systems. Furthermore, secure communication in time-division duplex multi-cell multi-user MaMIMO systems in the presence of a multi-antenna active eavesdropper has been studied in [56]. In the practical implementation of MaMIMO systems, secure transmission with the application of finite-resolution analog beamforming and a limited number of radio-frequency (RF) chains have been investigated in [54] and [57]. Furthermore, to address the issue of pilot contamination attacks, a secret key agreement protocol under the attack was established in [58], and the work in [59] proposed the encryption of the pilot sequence to hide it from the attacker. Subsequently, the potential for PLS in multi-user distributed massive MIMO systems was explored in [60]. Additionally, the authors in [61] focused on distributed massive MIMO system, investigating the power control scheme and the closed-form deterministic SINR equivalents.

In a subsequent study [62], an advanced approach for assessing legitimate data and AN was proposed. This technique aims to maximize the lower bound of the secrecy rate in multi-cell MaMIMO systems. However, this study found that legitimate users are subjected to AN leakage due to a design flaw in the precoders. This highlights the importance of designing precoders to meet system requirements. The work presented the derivation of the downlink secrecy rate in a relay-assisted MaMIMO system with the contribution of the proposed AN null-space precoder coupled with known precoders from [63]. Furthermore, a

study in [64] proposed a method of enhancing communication security over a fading wireless medium in the presence of a hidden eavesdropper. A portion of the available power was allocated for direct-broadcasting AN towards the eavesdropper. Moreover, the work in [65] studied the Rician Fading MaMIMO channels in the context of AN-aided jamming of Rician Fading massive MIMO channels. Regarding MaMIMO relaying, a comparison between two classic relaying schemes, including amplify-and-forward (AF) and decode-and-forward (DF) for PLS at the MaMIMO relay with imperfect CSI was presented in [66].

The previously mentioned works focus on evaluating the security performance of MaMIMO systems, demonstrating the lack of research on securing communications of CF-MaMIMO systems. Recently, a study in [67] applied PLS techniques in a CF-MaMIMO system. It formulated and evaluated a lower bound for the secrecy rate. Additionally, authors in [67] address issues concerning energy consumption and maximizing the achievable data secrecy rate.

2.3 Analyzing the Effect of HWIs

The works addressed to this point studied secure transmission in MaMIMO systems with the assumption that the transceivers' hardware is ideal. Furthermore, the authors do not consider the impact of HWIs within the context of MaMIMO systems. However, in real-world-scenarios, the wireless communication system experiences HWIs, including phase noise, power amplifier non-linearities, quantization errors, amplification noise and I/Q imbalance [68]. These HWIs are exacerbated in MaMIMO since the vast number of BS antennas/APs use low-cost hardware components to maintain budget limits for operators. Despite mitigating HWIs using compensation algorithms, residual HWIs remain due to time-varying randomness [35]. Moreover, these residual impairments are typically modelled as an additive Gaussian impairment with variance determined by the useful signal power [69]. Through analytical and experimental results, this model has been verified [69].

2.3.1 Performance of MaMIMO Systems

The impact of HWIs on MaMIMO has been studied in several works [70],[71],[72]. The work in [70] analyzed the effects of phase noise introduced by free-running oscillators on the downlink performance of MaMIMO systems with various linear precoder designs. Then, in [71], avoiding distortions generated by power amplifier linearities at the transmitter through constant envelope precoding in MaMIMO was explored. Moreover, the detrimental effects of HWIs introduced through different sources on MaMIMO systems was investigated in [35]. The residual HWIs were modeled as additive distortion noises. Considering a comprehensive residual HWIs model that comprises of multiplicative phase noise and additive distortion noise, the authors in [72] introduced closed-form expressions for achievable user data rates in uplink MaMIMO systems. The substantial degradation in performance of MaMIMO is evident in the previously mentioned works.

With the recent interest sparked by the study of HWIs in advanced wireless communication technologies, researchers have predominantly investigated the impact of HWIs in the context of MaMIMO system design and performance. The secrecy of communications has not been adequately studies in existing works [70] - [72]. However, considering security performance in the analysis presents a notable concern: while the legitimate user in the system employs low-cost hardware generating an increasing amount of HWIs, the eavesdropper potential employs high-quality, HWI-free equipment. This variation in hardware quality was not addressed in existing works related to PLS [51]- [67] neither in previous studies involving HWIs [70]- [72], therefore prompting the need of a new analysis and design framework. For instance, null-space AN precoding, which was widely known to improve the security of MaMIMO systems [62], [55], [73] is ineffective when the system is subject to phase noise. This initiated the motivation behind studying the effectiveness of security measures in the presence of HWIs. A study in [74] presents the effect of HWIs on the security of MaMIMO systems. It considers the joint impact of multiplicative phase noise and additive distortion noise. Additionally, the effect of phase noise on the secrecy performance of downlink MaMIMO systems has been investigated in [75].

2.3.2 Performance of CF-MaMIMO Systems

Although HWIs have detrimental effects, there is a limited number of works that have considered their impact in the context of CF-MaMIMO systems [76],[77], [78], [79]. In comparison to MaMIMO systems, CF-MaMIMO uses different computations for ZF and AN null-space beamforming. The authors in [76] employ a hardware distortion model to analyze the uplink and downlink performance of CF-MaMIMO considering a non-ideal transceiver. The derived closed-form spectral and energy efficiency expressions reveal the impact of the quantity and hardware quality factors of the APs and users on the system performance. Another work in [77] studies the uplink transmission of a front-haul constrained CF-MaMIMO system with residual HWIs at the users and APs. The effects of finite capacity front-haul links are investigated by deriving closed-form achievable data rates for encoding strategies. Additionally, they proposed low-complexity front-haul allocations and studied the sum spectral and energy efficiency of the system. Later, the achievable performance of CF-MaMIMO systems with low-resolution analog-to-digital converters at APs and users was explored in [78]. The study derived a closed-form expression for the achievable rate of each user. Furthermore, they propose an ADC resolution bits allocation algorithm to maximize the sum rate while adhering to the ADC resolution bits constraint. Additionally, a max-min power allocation method to improve user fairness is proposed. Similarly, the work in [79] considered the effect of HWIs at the APs and users and derived the closed-form expressions for the SE of the CF-MaMIMO system.

The earlier-mentioned works demonstrate the impact of HWIs on the system performance of CF-MaMIMO. However, they do not consider the effects of HWIs on the security performance. One of the very few works addresses the security performance of CF-MaMIMO in the presence of HWIs in [80]. The study considers residual additive HWIs over the Rayleigh fading channels in the case of spoofing attacks. Furthermore, by employing a hardware distortion model, they derived a Linear Mean-square Estimation channel estimator for the proposed model. The authors obtained a closed-form achievable ergodic secrecy rate expression to demonstrate the effect of HWIs on security performance. Furthermore, they

proposed a power control scheme for downlink transmission to maximize the achievable secrecy rate.

This work addresses limitations in [80], considering the following aspects: First, it carefully considers the impact of the non-idealities of transceivers' hardware in implementing PLS on MaMIMO systems. This involves performing beamforming computations and AN broadcasting, which has been demonstrated to be effective in mitigating eavesdropping attacks. Second, it not only considers the security performance but also analyzes the system performance of MaMIMO systems. In addition, it employs a generic model for HWIs to include any source of these impairments. Furthermore, it addresses the disparity in equipment quality among users, APs, and eavesdroppers. Overall, this work analyzes the security performance and system performance of CF-MaMIMO systems in the presence of HWIs.

This chapter provides a background of the fundamental concepts in this thesis, including the advantages of MaMIMO and CF-MaMIMO, as well as the security challenges posed by these systems. Moreover, the chapter reviews existing research on implementing PLS in MaMIMO systems. It also examines previous studies on the impact of HWIs on both system and security performance in CF-MaMIMO. Overall, the chapter underscores the need for comprehensive analysis to address the challenges posed by HWIs in current wireless communication systems.

Chapter 3

Mathematical Modelling

This chapter introduces a mathematical model for analyzing the CF-MaMIMO system. It provides a detailed description of the system model, encompassing the environmental setup and architectural components. The utilization of beamforming techniques for system protection is discussed. Furthermore, the chapter explores the impact of HWIs on communication systems, delving into their modelling and integration within the CF-MaMIMO system. Performance metrics such as SSR, USR, and ER are also highlighted for system evaluation.

3.1 The Cell-Free Massive MIMO System

3.1.1 System Model

In this paper, we consider a CF-MaMIMO system consisting of M number of APs serving K single-antenna users simultaneously in the presence of E eavesdroppers as illustrated in Fig. 3.1. The APs and users are randomly distributed over a wide geographical area, achieving $M \gg K$.

Within this setup, we consider a Non-Line-of-Sight environment where the signal travels via indirect paths, bouncing off surfaces or diffracting around obstacles. This results in substantial scattering between the APs and the user terminals. It is important to note that different sets of scatterers may exist for each AP and user. Consequently, the signal travels

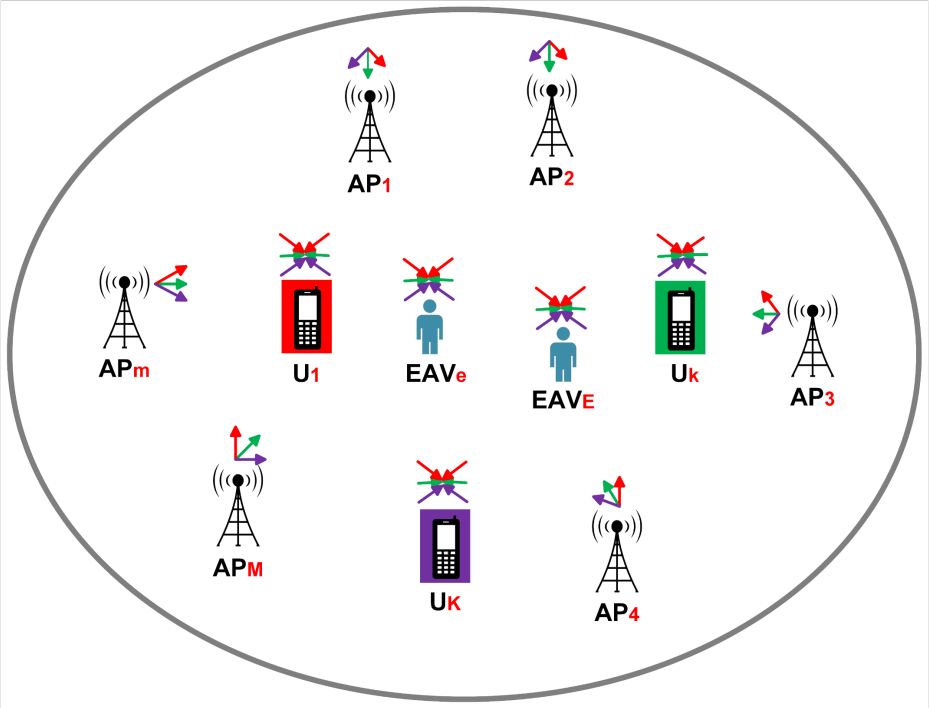

Fig. 3.1 Cell-Free Massive MIMO System

through numerous Non-Line-of-Sight paths to reach the receiver, resulting in a superposition of received signals that leads to either reinforcement or cancellation.

The channel coefficient between the m^{th} AP and the k^{th} user, h_{km} is expressed as

$$h_{km} = \sqrt{\beta_{km}}\alpha_{km} \tag{3.1}$$

where β_{km} is a positive real number denoting the large-scale fading coefficient. This coefficient encompasses the impact of distance-dependent path loss and shadowing. It evolves gradually, allowing accurate estimation and tracking. The large-scale fading coefficient is unique for each set of APs and users in the communication system. The second factor $\alpha_{\text{km}} \sim \mathcal{N}(0,1)$ represents the small-scale fading coefficient embodying the rapid fluctuations of amplitude and phase due to constructive and destructive interference of multi-path components. We assume these coefficients are independent and identically distributed (i.i.d) random variables. In this case, we consider the block fading model, i.e., we assume that these

coefficients remain constant within a coherent interval; however, they are independent over different coherent intervals.

Similarly, the channel gain h_{em} between eavesdropper and transmitter is given by:

$$h_{em} = \sqrt{\beta_{em}}\kappa_{em} \tag{3.2}$$

where β_{em} represents the large-scale fading coefficient relative to the eavesdropper and AP, and $\kappa_{\text{em}} \sim \mathscr{CN}(0,1)$ denotes the small-scale fading coefficient relative to the eavesdropper and AP.

3.1.2 Beamforming Strategy

To protect our system from eavesdroppers, we implement a beamforming technique in which the AP beamforms the data streams for legitimate users using the ZF approach, and broadcasts AN to the null of those legitimate users. The primary goal of beamforming is to enhance signal strength and mitigate interference by directing transmitted signals toward specific locations. In ZF beamforming, the aim is to eliminate interference that distorts the desired signal. This is accomplished by constructing a ZF beamforming matrix, denoted as $\mathbf{W}^{ZF}$ in such a way that when it is multiplied with $\mathbf{H}$, it results in an identity matrix $\mathbf{I}_K$, where K is the number of users. The ZF beamforming matrix can be represented as follows:

$$\mathbf{W}^{ZF} = \mathbf{H}^{\text{H}} \left(\mathbf{H}\mathbf{H}^{\text{H}}\right)^{-1},$$

where $\mathbf{H} \in \mathbb{C}^{K\times M}$ is the real channel matrix between M APs and K users, Additionally, the normalized beamforming vector $\mathbf{G} \in \mathbb{C}^{M\times K}$ for the k^{th} user is computed as:

$$\mathbf{G}_{(:,k)} = \frac{\mathbf{W}_{(:,k)}}{\|\mathbf{W}_{(:,k)}\|}. \tag{3.3}$$

The normalization of beamforming vectors is a crucial step in ensuring that the total power allocated to each user is uniform and satisfies the system's power constraints, resulting in enhanced system performance.

In wireless networks, AN-based transmission is recognized as an effective technique that can be implemented in PLS to ensure secure communication. This strategy intentionally degrades the channel quality of the eavesdropper by generating interference, which disrupts the eavesdropper's capabilities, hence securing confidential information. This AN is designed to lie in the null space of the legitimate user while being directed in the range space of the unintended user. This strategy is implemented such that the AN is nullified at the legitimate user while ensuring that only the eavesdropper's channel is degraded [8]. The generation of $\overline{d}$ AN streams is based on the AP's knowledge of the legitimate users' CSI, where the normalized beamforming vector for the AN signal, $\overline{\mathbf{G}} \in \mathbb{C}^{M \times \overline{d}}$, is obtained from the columns of $\mathbf{null}(\mathbf{H})$. It's important to note that the system possesses perfect CSI, allowing for accurate beamforming. We make this assumption for investigation purposes, ensuring that the degradation in the system is solely due to the impact of the HWIs rather than AN leakage from imperfect estimation.

3.2 Impact of HWIs on Communication Systems

Within wireless systems, hardware components often exhibit non-ideal behaviour, resulting in various non-idealities known as HWIs. These impairments include power amplifier non-linearities, finite-resolution quantization in analog-to-digital converters, phase noise in local oscillators, amplitude/phase imbalance in I/Q mixers, and sampling jitter [81]. Despite efforts to mitigate the effects of HWIs using compensation algorithms, residual impairments remain because of modelling inaccuracies and the inherently destructive nature of some impairments [81]. In this paper, we will not delve into the detailed modelling and compensation of HWIs; rather, we will focus on analyzing residual HWIs' effects.

3.2.1 Modeling HWIs

To investigate the effect of residual HWIs on communication, we adopt modeling non-idealities as non-linear memory-less filters at both the transmitter and receiver, demonstrated

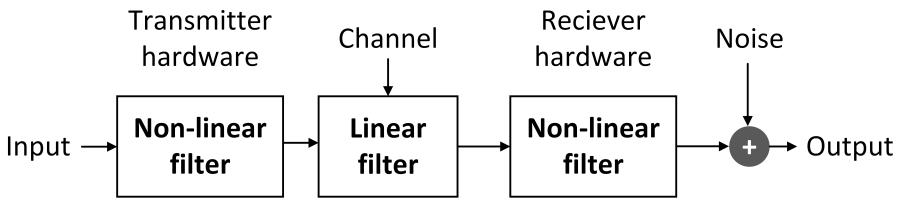

Fig. 3.2 Transceiver with HWIs Block Diagram.

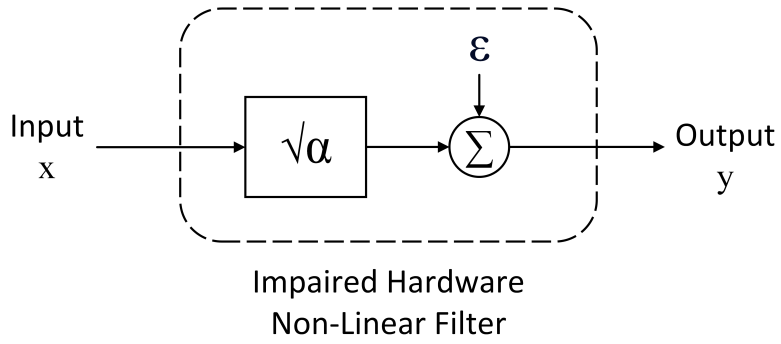

Fig. 3.3 Modelling of Hardware Impairments.

in Fig. 3.2. Introducing distortion into the transmitted signal involves representing HWIs by a nonlinear function as depicted in Fig. 3.3.

This nonlinear function is expressed as:

$$y = \sqrt{\alpha}x + \varepsilon, \tag{3.4}$$

where $x \sim CN(0,p)$ is the input signal, and ε is the distortion term. In the worst-case scenario where the HWIs are independent of the input signal, their probability distribution is given by $\varepsilon \sim CN(0,(1-\alpha)p)$, and their power is proportional to the input power p, with a scaling factor of $(1-\alpha)$. The distortion term is characterized by $\alpha \in (0,1]$ which represents the hardware quality factor, where $\alpha = 1$ corresponds to ideal hardware components, and $\alpha = 0$ represents the pathological scenario where the output signal is uncorrelated with the input. It is important to note that, as per definition, $\mathbb{E}\{|y|^2\} = \alpha p + (1-\alpha)p = p$ for any α.

3.2.2 Applying PLS and Integrating HWIs into the System

The signal transmitted by the m^{th} AP, $x_m \in \mathbb{C}^{M\times 1}$ is represented by:

$$x_m = \sqrt{p_d \alpha_m}\mathbf{G}_{(m,:)}\mathfrak{D}^{\frac{1}{2}}_{(:,m)}\mathbf{s} + \sqrt{\overline{p_d}\alpha_m}\ \overline{\mathbf{G}}_{(m,:)}\,\overline{\mathbf{s}} + \varepsilon_m. \tag{3.5}$$

The first term is referred as the desired signal where p_d is the power budget, α_m signifies the hardware scaling factor associated with the m^{th} AP, $\mathbf{G}$ is the normalized beamforming matrix referenced in (3.3), $\mathbf{s} \in \mathbb{C}^{K\times 1}$ which satisfies $\mathbb{E}\{ss^H\} = I_K$ is a vector of K symbols intended for the k^{th} user and η_{km} are power control coefficients that are selected to satisfy the specified power constraints at each AP given as:

$$E\left\{|x_m|^2\right\} \leq p_d \tag{3.6}$$

and

$$\text{TR}\left(\mathbf{G}_{(m,:)}\mathfrak{D}_{(m,:)}\mathbf{G}^{\text{H}}_{(m,\beth)}\right) \leq 1 \quad \text{for all } m \tag{3.7}$$

These constraints ensure that the total transmitted power of each AP is not greater than p_d. The power coefficients related to the m^{th} AP are stored in the power coefficient matrix $\mathfrak{D}_{(m,:)} \in \mathbb{R}^{K\times K}$. Furthermore, the power coefficient matrix $\mathbf{D} \in \mathbb{R}^{K\times M}$contains all the non-negative power control coefficients η_{km}.

The second term is descibed as AN where $\overline{p}_d$ is the AN power, and $\overline{\mathbf{s}} \in \mathbb{C}^{\overline{d}\times 1}$ is such that $\overline{d}$ is the number of AN streams. Lastly, ε_m is a distortion term related to HWIs at the APs. The distortion term at the m^{th} AP is defined by:

$$\varepsilon_m \sim CN(0,(1-\alpha_m)(p_d+\overline{p_d})), \tag{3.8}$$

while the vector of HWIs related to all APs is given as:

$$\bar{\varepsilon}_m = \left[\varepsilon_1,\cdots,\varepsilon_m\right]^{\text{T}}. \tag{3.9}$$

The received signal at the k^{th} user is expressed as:

$$
\begin{aligned}
y_k =& \sqrt{p_d}\sqrt{\alpha_m}\sqrt{\alpha_k}\mathbf{H}_{(k,:)}\mathfrak{D}^{\frac{1}{2}}_{(k,:)}\mathbf{G}_{(:,k)}s_k \\
&+ \sqrt{p_d}\sqrt{\alpha_m}\sqrt{\alpha_k}\sum_{i=1,i\neq k}^{K}\mathbf{H}_{(k,:)}\mathfrak{D}^{\frac{1}{2}}_{(i,:)}\mathbf{G}_{(:,i)}s_i \\
&+ \sqrt{\alpha_k}\mathbf{H}_{(k,:)}\bar{\varepsilon}_m + \varepsilon_k + n_k. \qquad (3.10)
\end{aligned}
$$

The first term represents the desired signal where $\mathfrak{D}_{(:,k)} \in \mathbb{C}^{M\times M}$ is a diagonal matrix of power coefficients for the k^{th} user, s_k is user k's data signal. $\mathbf{G}_{(:,k)}$ is the normalized beamforming vector for the k^{th} user. During each coherence block, the normalization process ensures that the constraint given by $E\|G(:,k)\|^2 = 1$ is achieved. Furthermore, it ensures that the total power allocated to the k^{th} user is equivalent to $p_d\sum_{m=1}^{M}\eta_{km}$.

The second term is defined as the interference signal where α_k is the hardware scaling factor for the k^{th} user, and the next two terms take into account the distortion in the system. Here, ε_k is a distortion term related to HWIs at the users, given by:

$$\varepsilon_k \sim CN(0, P_{rk}(1-\alpha_k)), \qquad (3.11)$$

where the power at the receiver at the user, P_{rk}, is represented by:

$$P_{rk} = \sum_{m=1}^{M}|h_{km}|^2\left[p_d + \overline{p_d}(1-\alpha_m)\right], \qquad (3.12)$$

while the final term, n_k, is Additive White Gaussian Noise (AWGN) for the k^{th} user.

To determine the quality of the user signal, we can derive the signal-to-interference-plus-noise ratio for the k^{th} user (SINR$_k$) expressed in (3.13) in the top of the next page. SINR$_k$ evaluates the strength of the received signal considering interference and noise present in the system. The numerator of the SINR$_k$ equation comprises the power of the desired signal, and the denominator consists of interference from other users, hardware distortions, receiver noise, and power constraints. Overall, the SINR$_k$ is essential for evaluating the performance of the communication system.

$$\text{SINR}_k = \frac{p_d \alpha_m \alpha_k \left| \mathbf{H}_{(k,:)} \mathfrak{D}_{(k,:)}^{1/2} \mathbf{G}_{(:,k)} \right|^2}{p_d \alpha_m \alpha_k \sum_{i=1, i\neq k}^{K} \left| \mathbf{H}_{(k,:)} \mathbf{D}_{(i,:)}^{1/2} \mathbf{G}_{(:,i)} \right|^2 + \alpha_k \left| \mathbf{H}_{(k,:)} \bar{\varepsilon}_m \right|^2 + P_{rk}(1-\alpha_k) + \sigma_w^2} \tag{3.13}$$

Lastly, the received signal at the eavesdropper, y_e, is:

$$\begin{aligned} y_e = & \sqrt{p_d}\sqrt{\alpha_m}\sqrt{\alpha_e} \sum_{m=1}^{M} h_{em} \mathbf{G}_{(m,\,:)} \mathfrak{D}_{(:,m)}^{\frac{1}{2}} \mathbf{s} \\ & + \sqrt{\overline{P_d}}\sqrt{\alpha_m}\sqrt{\alpha_e} \sum_{m=1}^{M} h_{em} \overline{\mathbf{G}}_{(m,:)} \bar{\mathbf{s}} \\ & + \sqrt{\alpha_e} \mathbf{H}_{em} \bar{\varepsilon}_m + \varepsilon_e + n_e \end{aligned} \tag{3.14}$$

Here, the first term represents the intercepted signal, the second term is the AN at the eavesdropper, and the next two terms consider the distortion generated by the AP as well as the eavesdropper.

The distortion term representing the HWIs for the eavesdropper, ε_e, is expressed as:

$$\varepsilon_e \sim CN(0, P_{re}(1-\alpha_e)), \tag{3.15}$$

where the power at the eavesdropper is given by:

$$P_{re} = \sum_{m=1}^{M} \left(p_d + \overline{p_d}\right) |h_{em}|^2 . \tag{3.16}$$

and the AWGN at the eavesdropper is n_e.

To evaluate the strength of the eavesdropped signal, we derive the signal-to-noise ratio for the eavesdropper (SNR_e) in (3.17).

$$\text{SNR}_e = \frac{p_d \alpha_m \alpha_e \sum_{m=1}^{M} \left| h_{em} \mathbf{G}_{(m,:)} \mathbf{D}_{(:,m)}^{1/2} \right|^2}{\bar{p}_d \alpha_m \alpha_e \sum_{m=1}^{M} \left| h_{em} \bar{\mathbf{G}}_{(m,:)} \right|^2 + \alpha_e \left| H_{em} \bar{\varepsilon}_m \right|^2 + P_{re}(1-\alpha_e) + \alpha_w^2} \tag{3.17}$$

The SNR_e compares the intercepted signal to the combined effects of noise and interference. The numerator includes the power of the intercepted signal, and the denominator consists of noise, hardware distortions, and power constraints.

Overall, the effect of HWIs on the quality of the system is captured by the distortion terms (ε_m, ε_k, ε_e). These terms are often modelled as Gaussian noise with variances determined by the corresponding hardware scaling factors. The power at the receiver (P_{rk}) and the power at the eavesdropper (P_{re}) represent the signal power incorporating the impact of HWIs.

3.3 Evaluation Metrics

The security performance of the system is evaluated by the SSR which determines the maximum achievable rate at which confidential information can be transmitted without eavesdropper interception. SSR is calculated as the difference between the USR and ER. Mathematically, it is expressed as:

$$\text{SSR} = \max(0, \text{USR} - \text{ER}), \tag{3.18}$$

where,

the USR is given by

$$\text{USR} = \tau \sum_{k=1}^{K} \log_2(1 + \text{SINR}_k), \tag{3.19}$$

USR is the sum of individual user rates. It is determined by the SINR_k and τ which is the ratio of downlink data samples relative to the number of samples per coherence block.

The eavesdropper rate is determined by the SNR_e and τ, and is expressed as

$$\text{ER} = \tau \log_2(1 + \text{SNR}_e), \tag{3.20}$$

The chapter provides a mathematical model for the CF-MaMIMO system, detailing its system model and beamforming strategy. It involves the modeling and integration of HWIs into the CF-MaMIMO. Additionally, it discusses the application of PLS techniques and outlines metrics such as the SSR, USR, and ER to assess system performance.

Chapter 4

Simulation and Results

This chapter commences with a detailed overview of the CF-MaMIMO system, followed by an extensive exploration of its secrecy and overall performance. Subsequently, it undertakes a comprehensive analysis of HWIs across various scenarios: increasing transmitted power, expanding the number of APs, and elevating AN levels. Each analysis thoroughly examines the effects of varying the hardware quality of users, eavesdroppers, and APs individually, offering valuable insights into their respective influences on system behavior.

4.1 System Construction

In this section, we study the impact of HWIs on a CF-MaMIMO system. Additionally, we evaluate PLS techniques by integrating them into the CF-MaMIMO system, as detailed in [82]. The system consists of $M = 64$ single-antenna APs, $K = 16$ single-antenna users, and $E = 8$ eavesdroppers, which are uniformly distributed over a $1000\,\mathrm{m} \times 1000\,\mathrm{m}$ coverage area. In this simulation, the results are generated over 1000 random systems; one of these systems is illustrated in Fig. 4.1.

The large-scale coefficient is modelled using the Hata-COST propagation model given by:

$$10\log_{10}(\beta_{km}) = -136 - 35\log_{10}(d_{km}) + X_{km} \tag{4.1}$$

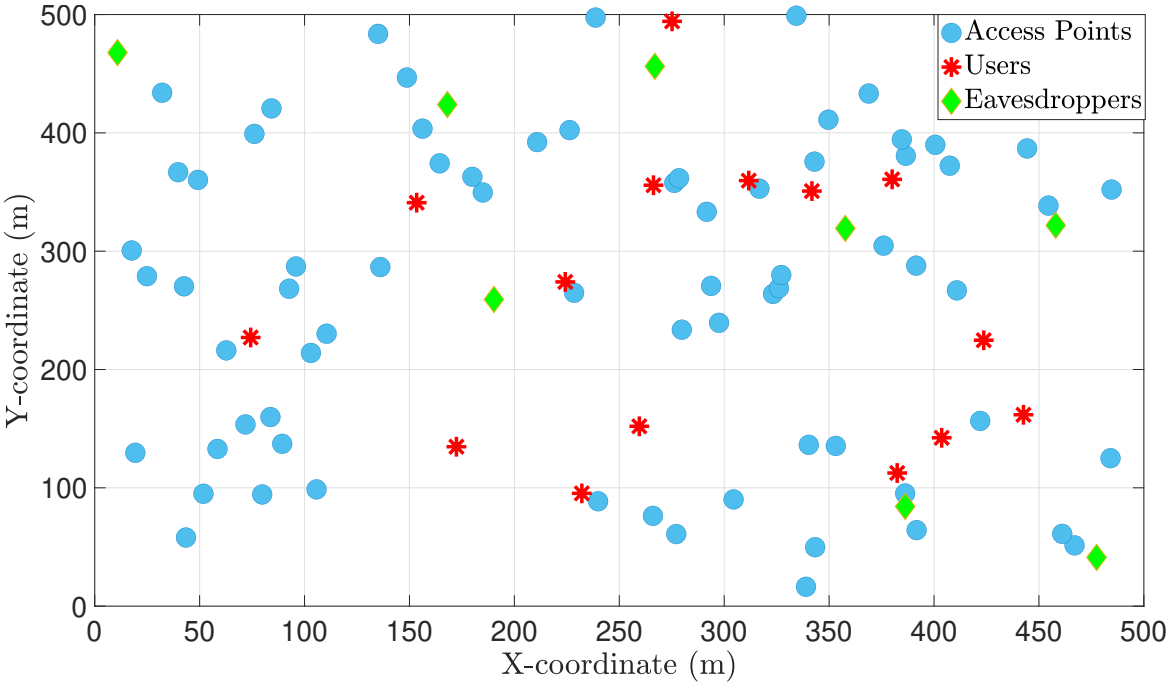

Fig. 4.1 Locations of APs, Users and Eavesdroppers.

In this case, d_{km} denotes the distance (in kilometers) between the m^{th} AP and the k^{th} user, and $X_{km} \sim \mathscr{CN}(0, \alpha^2_{\text{shadow}})$ is the shadow fading with $\alpha_{\text{shadow}} = 8\,\text{dB}$. The AWGN variance at each receiver is given by $\alpha_w^2 = T_0 \times K_B \times BW \times NF$, where $T_0 = 290\,K$ is the noise temperature, $KB = 1.381 \times 10^{-23}\,\text{J/K}$ is the Boltzmann constant, $BW = 20\,\text{MHz}$ is the bandwidth, and $NF = 9\,\text{dB}$ is the noise figure.

4.2 Analyzing System and Secrecy Performance

In this section, an investigation is conducted on the implications of varying different parameters on the performance and security of the CF-MaMIMO system, as illustrated through graphical representations. During the analysis, the effects of increasing transmitted power, the number of APs, and AN levels on the USR, ER and SSR are examined. The hardware scaling factors are varied for one communication terminal at a time to isolate the effects of the hardware quality of the users, eavesdroppers and APs. Consequently, the two terminals that are not being varied are assumed to have $\alpha = 0.995$.

4.2.1 Analyzing the Impact of HWIs with Increasing Transmitted Power

In wireless communications, an effective strategy for enhancing system performance is by increasing transmitted power. Boosting transmitted power provides numerous advantages that contribute to overall system improvement. Hence, this section examines the impact of increasing transmitted power on the USR and ER under different hardware quality conditions. The total AN transmission is maintained at 30 W for all the APs in the system.

Varying User Hardware Quality

Fig. 4.2 depicts the trends in the data rates of users and eavesdroppers with varying hardware quality conditions and increments in transmitted power. In this case, the hardware quality of the user is varied across scaling factor values $\alpha_k = 0.99, 0.995, 1$, and the hardware quality of the eavesdroppers and APs is considered $\alpha = 0.995$. In accordance with Fig. 4.2, increasing the transmitted power results in a proportional enhancement in USR. This enhancement is attributed to the increase in SINR_k with increments in transmitted power, as observed in Fig. 4.3. Moreover, the increase in transmitted power results in more reliable data transmission, thereby enhancing system performance. Furthermore, this observation aligns with the theoretical expressions mentioned in section 3.2.2. Observing the SINR_k equation (3.13) reveals the proportional relationship between SINR_k and p_d. Increasing p_d directly increases the SINR_k due to the presence of p_d in the signal power of the user. Based on Fig. 4.4, this is attributed to the faster rate of increase in signal power relative to that of HWIs and users' interference as transmitted power increases. Furthermore, the gap between the three plots for SINR_k and USR is attributed to the difference in hardware quality of the user. As the hardware quality approaches ideal conditions, the magnitude of the USR increases. Overall, increasing the transmitted power improves the USR under all user hardware conditions.

However, incrementing transmitted power also leads to an enhancement in the ER. In practical terms, this implies that increased transmitted power can potentially enhance the eavesdropper's ability to intercept communication signals.

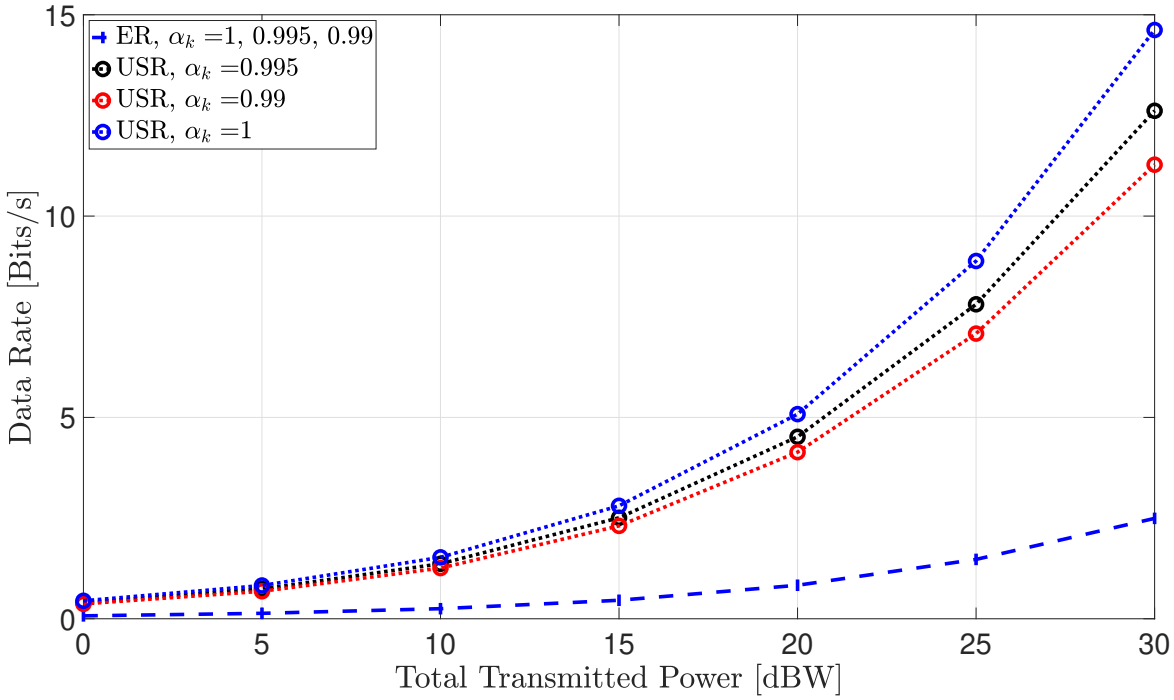

Fig. 4.2 Data Rate vs. Total Transmitted Power with Variable α_k, and $\alpha_m = \alpha_e = 0.995$.

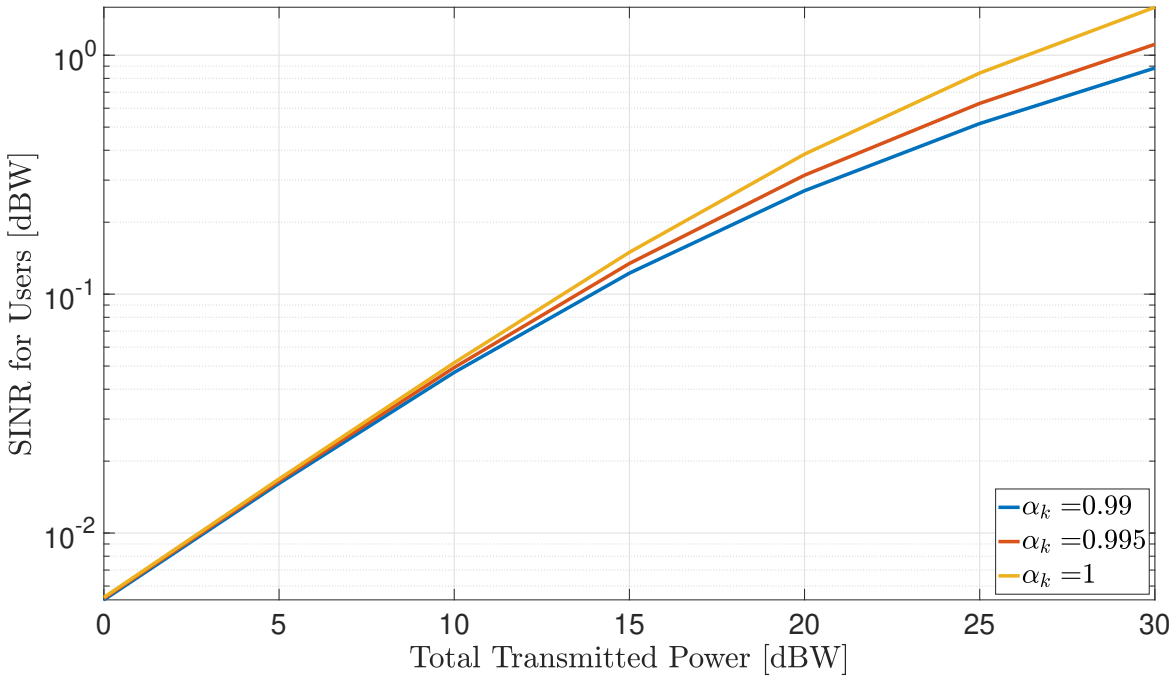

Fig. 4.3 SINR$_k$ vs. Total Transmitted Power with Variable α_k, and $\alpha_m = \alpha_e = 0.995$.

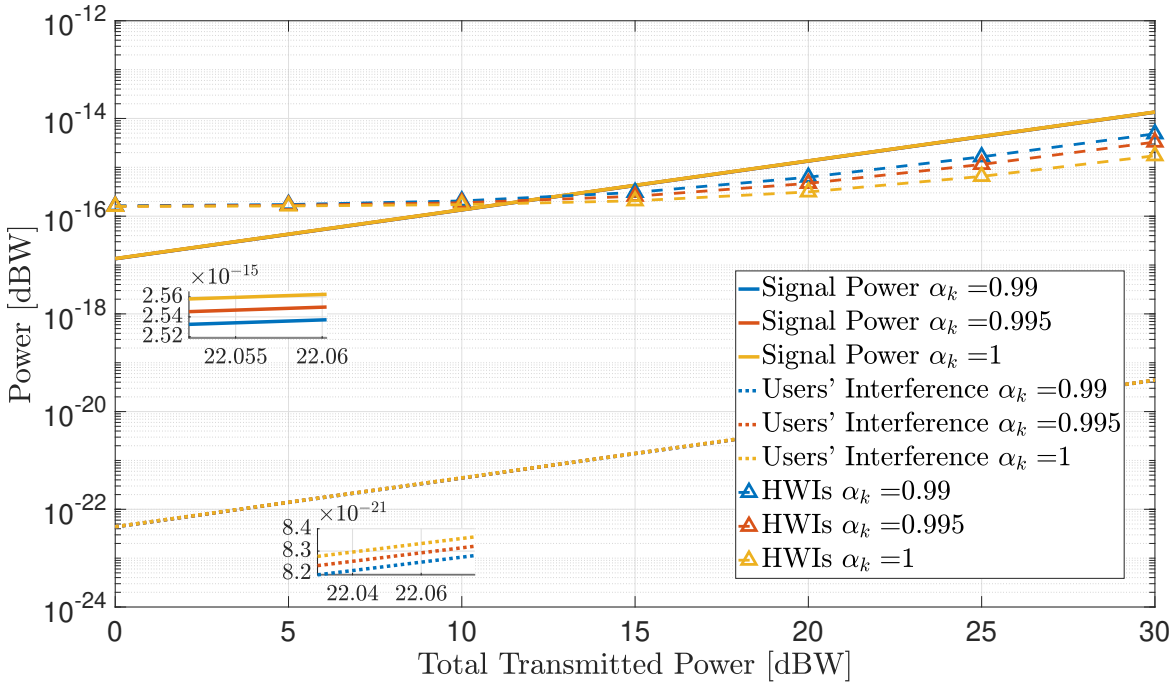

Fig. 4.4 User Signal Power, Users' Interference and HWIs as a function of Total Transmitted Power with Variable α_k, and $\alpha_m = \alpha_e = 0.995$.

Varying Eavesdropper Hardware Quality

Analyzing Fig. 4.5 demonstrates the influence of HWIs and fluctuations in transmitted power on the transmission rates of users and eavesdroppers. It delves into the specific effects of various hardware conditions of the eavesdropper, considering hardware scaling factors $\alpha_e = [0.99, 0.995, 1]$. To exclusively study the impact of varying eavesdropper hardware quality, the equipment of the users and APs is assumed to have $\alpha = 0.995$. As depicted in Fig. 4.5, the USR demonstrates a noticeable upward trend with elevating transmitted power levels. While the increase in transmitted power results in an enhancement in system performance, it also improves the eavesdropper's ability to intercept confidential data signals. Moreover, the ER depends on the quality of the eavesdroppers' channel along with the eavesdroppers' hardware quality. As shown in Fig. 4.5, ER inclines as the transmitted power increases. This occurs because ER depends on SNR_e; hence, when the transmitted power is raised, causing an improvement in SNR_e, it also results in an increase in ER, as illustrated in Fig. 4.6. Furthermore, by examining Fig. 4.7, it is evident that with elevating transmitted power levels,

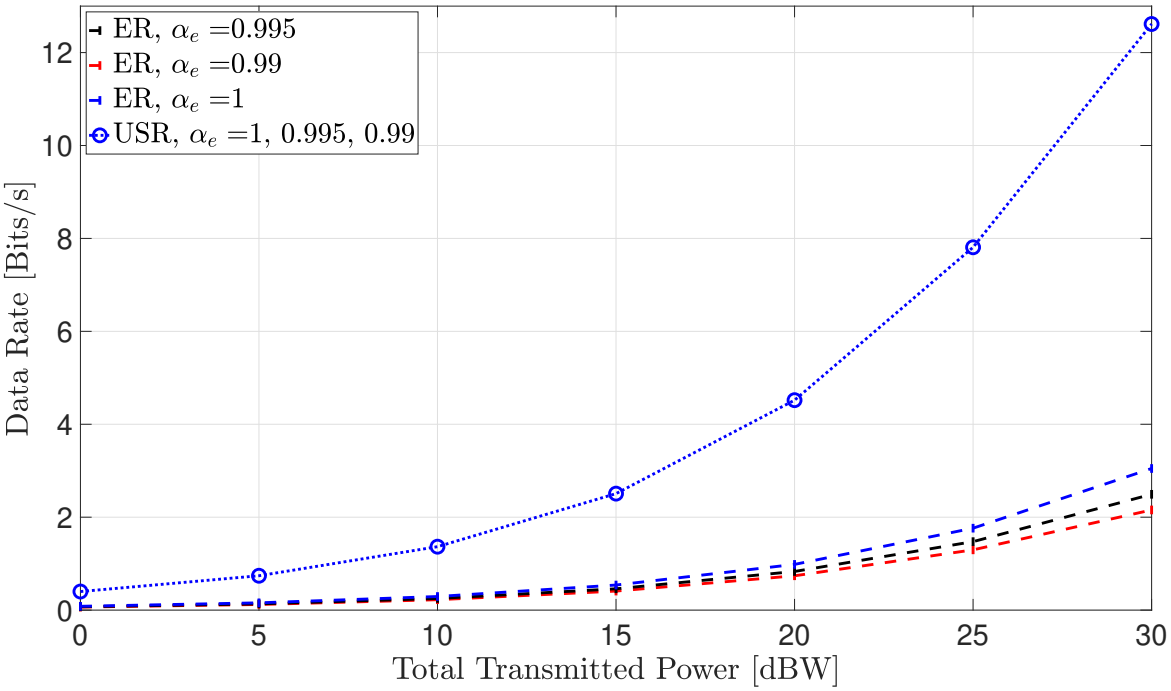

Fig. 4.5 Data Rate vs. Total Transmitted Power with Variable α_e, and $\alpha_m = \alpha_k = 0.995$.

the HWIs at the eavesdroppers and signal power of the eavesdroppers exhibit an upward trend. Moreover, the slope of the eavesdropper signal power is greater than that of HWIs at the eavesdroppers. Consequently, the increase in SNR_e is proportional to the increase in signal power as the transmitted power rises. Observing equation (3.17) reveals the presence of the variable p_d in the signal power of the eavesdropper as well as the HWIs terms in the denominator. However, due to the greater slope of the signal power, the impact of raising p_d on the signal power of the eavesdropper takes precedence. Therefore, as depicted in Fig. 4.6, an increase in the transmitted power results in an enhancement in SNR_e and, consequently, ER. With reference to Fig. 4.6 and Fig. 4.3, the SNR_e exhibits a more gradual increase with increments in transmitted power when the hardware quality of the eavesdropper is varied in this section compared to when the user hardware quality is altered in section 4.2.1. The slower increase in SNR_e in the case of fluctuations in the eavesdroppers' hardware quality is attributed to the AN broadcasted towards the null of the users. Additionally, higher hardware quality correlates with improved signal reception, resulting in higher values for both USR and ER.

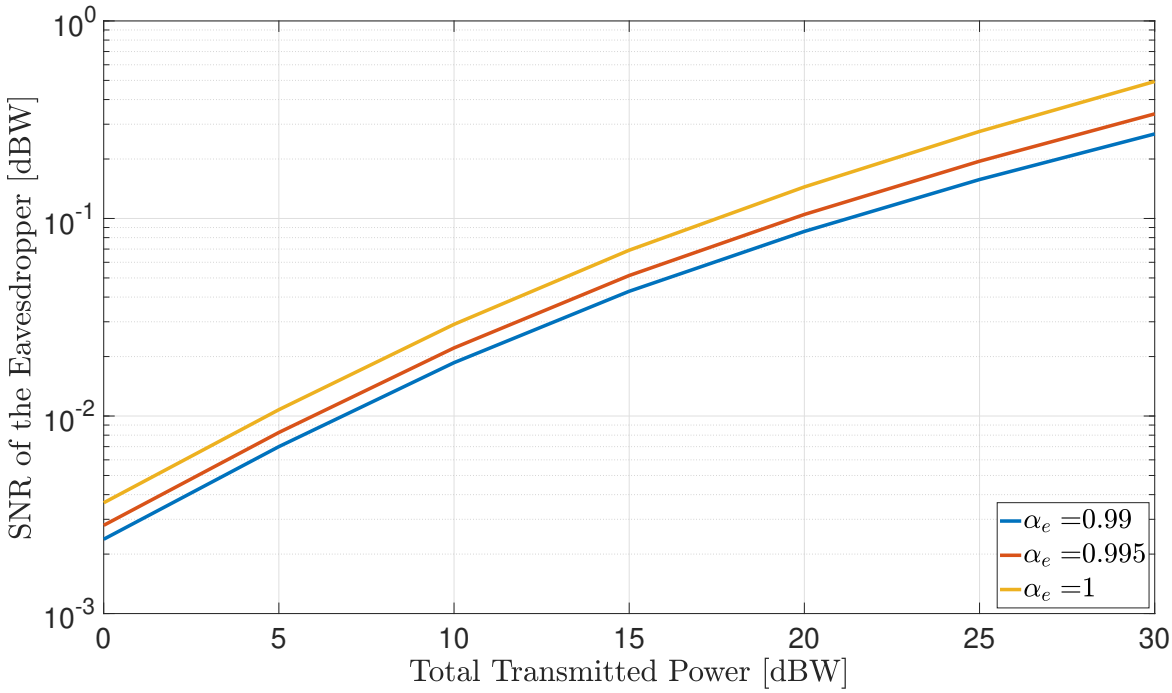

Fig. 4.6 SNR_e vs. Total Transmitted Power with Variable α_e, and $\alpha_m = \alpha_k = 0.995$.

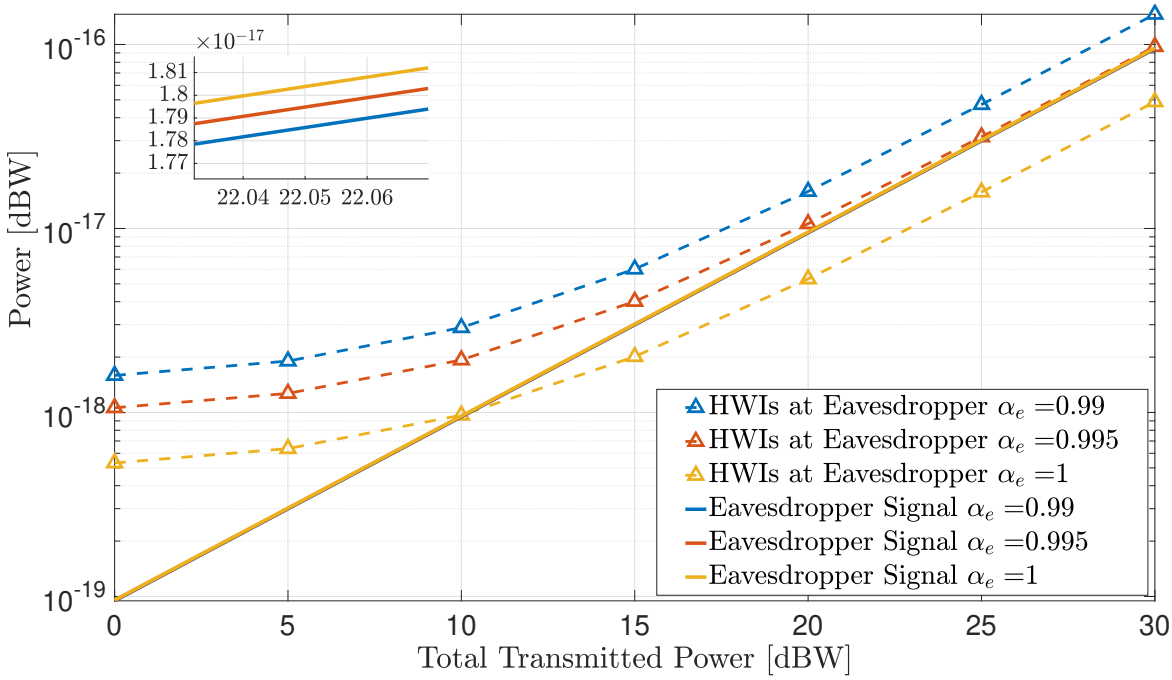

Fig. 4.7 Eavesdropper Signal Power and HWIs as a function of Total Transmitted Power with Variable α_e, and $\alpha_m = \alpha_k = 0.995$.

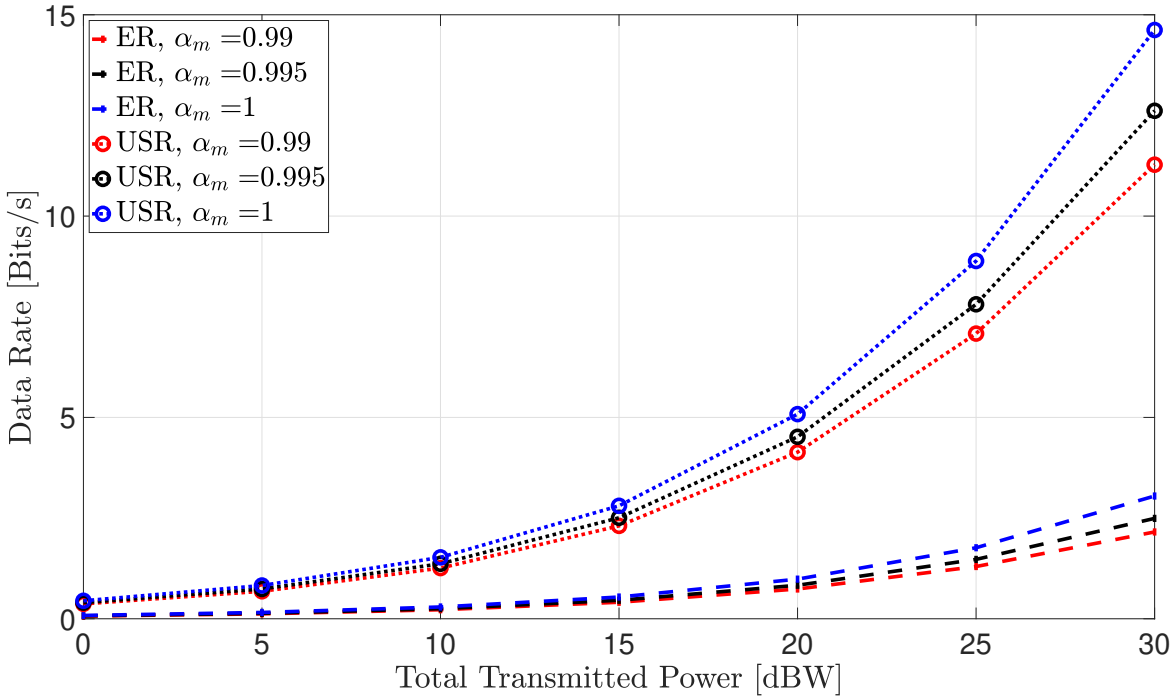

Fig. 4.8 Data Rate vs. Total Transmitted Power with Variable α_m, and $\alpha_k = \alpha_e = 0.995$.

Varying AP Hardware Quality

To investigate the effect of the HWIs at the AP, the hardware quality is varied for three different values of α, including 0.99, 0.995 and 1. The hardware quality of the users and eavesdroppers is considered to have $\alpha = 0.995$. Based on Fig. 4.8, it is evident that USR rises as the transmitted power increases. This rise in USR is attributed to the improvement in the signal strength of the user corresponding to higher SINR_k values. Observing Fig. 4.9 reveals the dependency of HWIs, users' interference and signal power of the user on the transmitted power. Furthermore, it is apparent that the rate of increase for the signal power surpasses that of the users' interference and HWIs as transmitted power levels increase. Due to this reason, the trend of the signal power of the user takes precedence in the SINR_k. Therefore, as the transmitted power increases, the signal power of the users increases, leading to an incline in SINR_k and USR. It's important to emphasize that when $\alpha_m = 1$, only the hardware impairment of the user contributes to the SINR_k. Fig. 4.8 also illustrates the fluctuations in ER with increasing transmitted power, demonstrating a slight incline.

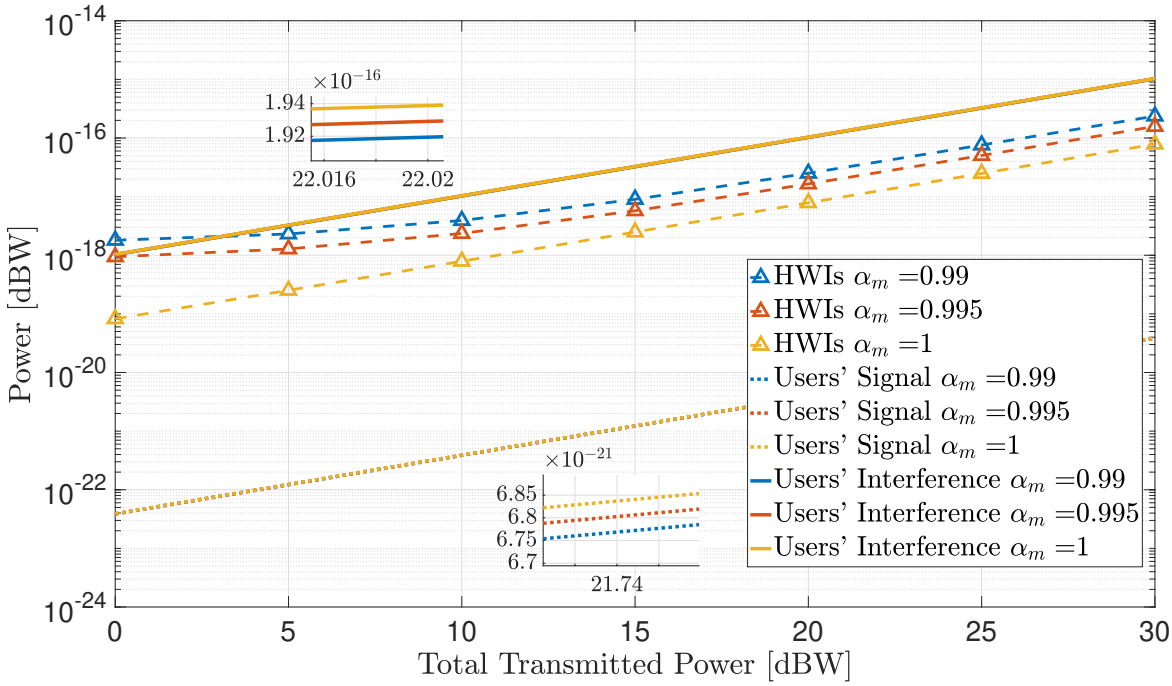

Fig. 4.9 User Signal Power, Users' Interference and HWIs as a function of Total Transmitted Power with Variable α_m, and $\alpha_k = \alpha_e = 0.995$.

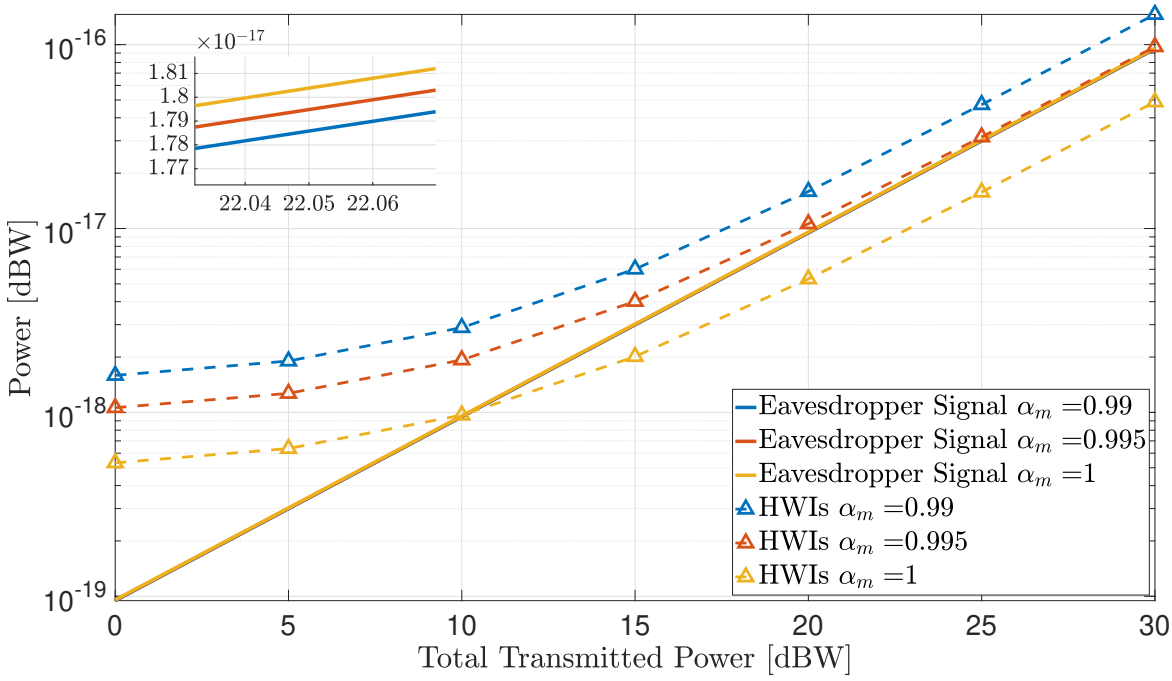

Fig. 4.10 Eavesdropper Signal Power and HWIs as a function of. Total Transmitted Power with Variable α_m, and $\alpha_k = \alpha_e = 0.995$.

Upon observing SNR_e equation, it is evident that the transmitted power is present in the signal power and HWIs. These HWIs increase with elevating transmitted power levels. Additionally, increments in transmitted power increase the signal power of the eavesdropper. It is evident that the rate of increase in eavesdroppers' signal power relative to transmitted power accelerates more rapidly than that of HWIs, as depicted in Fig. 4.10. Therefore, the SNR_e follows the trend of the eavesdroppers' signal power. Given the proportional relationship between SNR_e and the signal power of eavesdroppers, as the signal power of eavesdroppers increases with rising transmitted power, SNR_e will also increase.

In section 4.2.1, an in-depth investigation is conducted on the impact of increasing transmitted power on the performance of the CF-MaMIMO system. The analysis reveals that the key benefit of increasing transmitted power is an enhancement in USR. However, elevating transmitted power levels also result in a simultaneous enhancement in ER, indicating an increase in the tapped data by the eavesdropper. Additionally, the noise and interference levels elevate with increments in transmitted power. This underscores the significance of striking a balance between improving the user signal quality while ensuring minimum eavesdropper interception. Thus, the transmitted power is selected to achieve a suitable SNR at the receiver to ensure reliable communication. Practical considerations such as energy efficiency should also be taken into account since energy consumption increases with the transmitted power. Therefore, although increasing the transmitted power improves the system performance, trade-offs and practical considerations are necessary in selecting the transmitted power.

4.2.2 Examining the Effects of HWIs with the Deployment of Additional APs

To further enhance system performance, additional antennas are deployed in the network. This analysis examines the effects of increasing the number of antennas on the data rates of users and eavesdroppers. Additionally, the impact of the hardware quality of each communication terminal is investigated. In this study, the hardware scaling factors are adjusted individually

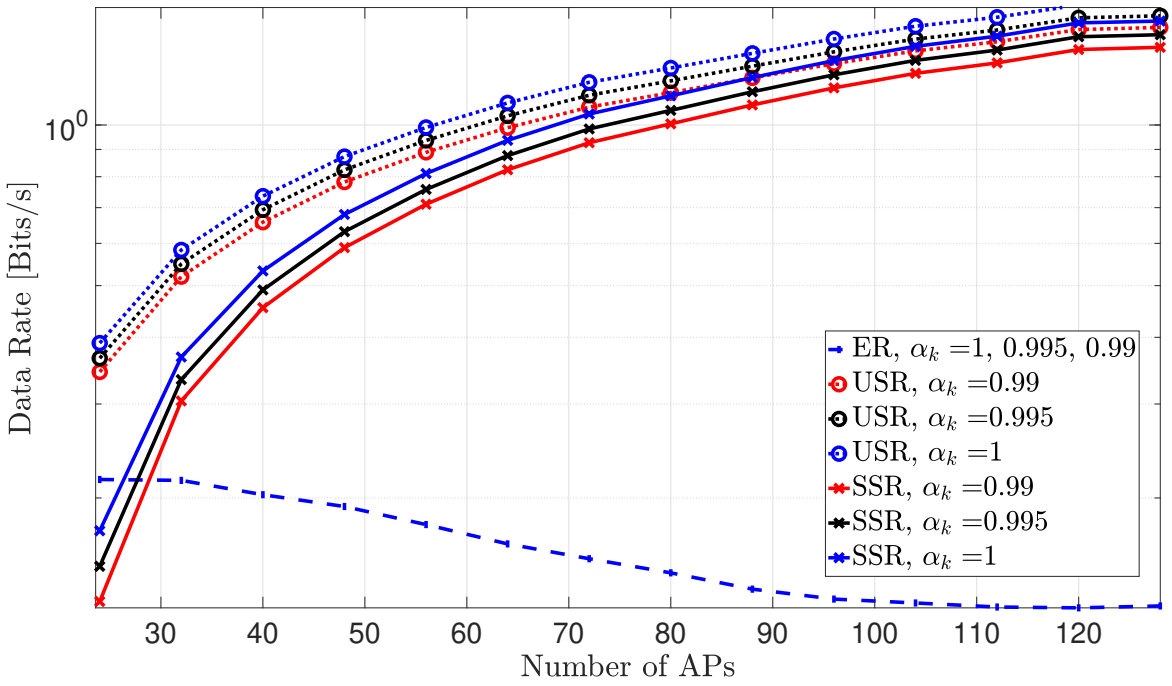

Fig. 4.11 Number of APs Vs. Data Rates with Variable α_k, and $\alpha_m = \alpha_e = 0.995$.

for one communication terminal at a time while maintaining the factors for the other two terminals at $\alpha = 0.995$.

Varying User Hardware Quality

Fig. 4.11 presents the impact of imperfections in the user's hardware while expanding the deployment of APs on the system and security performance. For this evaluation, the users' hardware quality, α_k, is varied across a range of values [0.99, 0.995, 1], while the hardware scaling factors for the eavesdropper and AP are fixed at $\alpha_e, \alpha_m = 0.995$. As depicted in Fig. 4.11, the USR increases with the growing number of APs. This enhancement in USR is attributed to an improvement in the SINR_k through enhanced beamforming techniques. Another reason for the improvement in USR is the increase in AP density since transmission distances and path losses decrease, facilitating more efficient signal transmission. Moreover, the incline in USR is more pronounced under ideal hardware conditions since there is no distortion due to HWIs produced by the user.

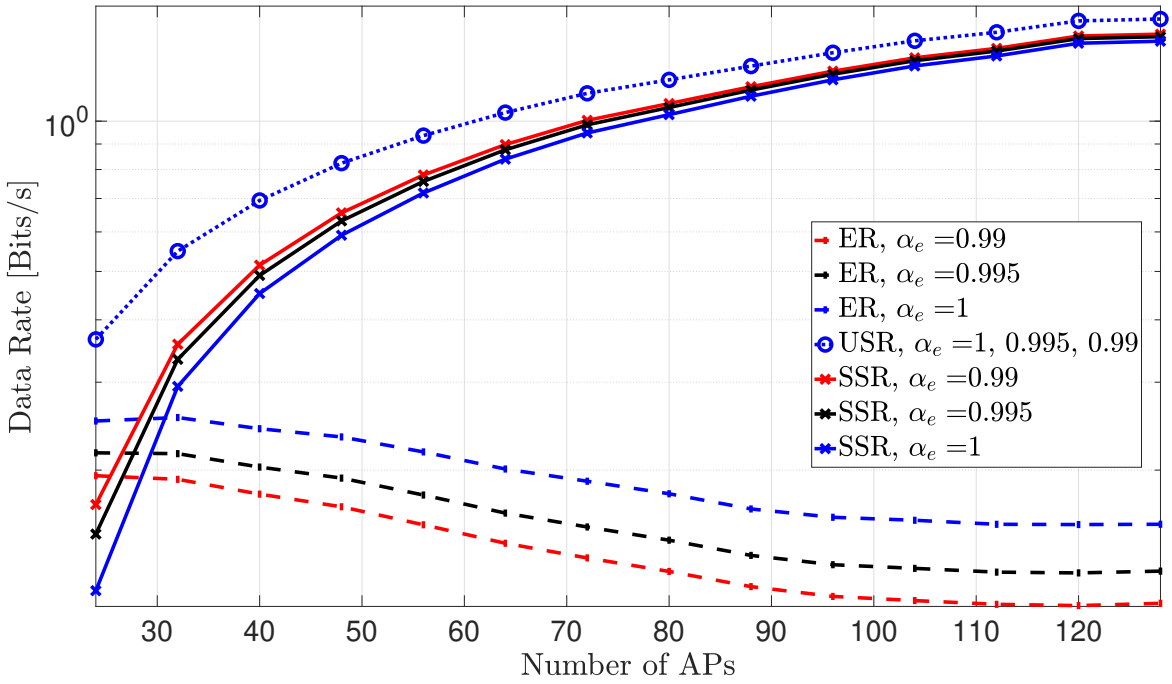

Fig. 4.12 Number of APs Vs. Data Rates with Variable α_e, and $\alpha_m = \alpha_k = 0.995$.

In contrast to USR, the ER declines as more APs are deployed, indicating reduced data interception by the eavesdropper. This decline is attributed to more effective beamforming of AN towards the null of the users wherein the eavesdroppers lie. Regardless of the hardware quality conditions of the user, the SSR inclines with the rise of AP numbers. This is due to the consistent reduction in intercepted data and stronger received signals for legitimate users enabling more secure transmission of confidential information. A notable observation is that as the hardware quality of the users approaches ideal conditions, the amplitude of the USR is greater since the user receives stronger signals. This increase in USR corresponds to an enhancement in SSR, thus SSR is highest under ideal hardware conditions.

Varying Eavesdropper Hardware Quality

Analyzing Fig. 4.12 entails a thorough exploration of the impact of HWIs and the addition of antennas on the transmission rates of users and eavesdroppers. This analysis particularly delves into the effects of different hardware conditions of the eavesdropper, characterized by $\alpha_e = [0.99, 0.995, 1]$. The hardware quality factor of the user and APs are set as $\alpha_k, \alpha_m =$

0.995. Upon observation of the trends illustrated in Fig. 4.12, it becomes evident that when $\alpha_e = 1$, the USR consistently increases as the number of APs increases. There are two key factors that contribute to this enhancement in SINR_k and, consequently, USR. Firstly, adding more antennas improves the robustness of beamforming techniques, resulting in stronger signals directed towards users. Secondly, there is a reduction in the distance between the transmitter and receiver in the case of an increased quantity of APs, as explained earlier in section 4.2.2. This reduction in transmission distance lessens the effects of shadow-fading. Overall, these factors contribute to improving SINR_k and, hence, enhancing the USR.

On the contrary, the ER declines as the number of APs increases. This decline indicates that the eavesdropper intercepts less data as the number of APs grows. This decline is attributed to enhancing the APs' beamforming capabilities as more APs are deployed, there is more effective broadcasting of AN towards the nulls of users. Moreover, the decline in ER is more pronounced under non-ideal hardware conditions. In such scenarios, additional noise and distortion introduced by HWIs exacerbate the decrease in ER compared to ideal conditions. This decline in ER indicates better protection against eavesdroppers in the system. With the substantial incline in USR and decrease in ER, SSR increases significantly, implying enhanced system security. In other words, the strength of the received signals for legitimate users is enhanced, and interference is reduced; the system's ability to transmit secret information securely improves, leading to a higher SSR. Overall, as the number of APs increases, SSR increases under all hardware quality conditions of the eavesdropper. A key observation is that as the hardware quality of the eavesdroppers approaches ideal conditions, the amplitude of the ER is greater since the eavesdropper is able to tap more data. This increase in ER corresponds to a decrease in SSR; thus, SSR is lowest under ideal hardware conditions.

Varying AP Hardware Quality

Overall, in this analysis, it has been demonstrated that increasing the amount of antennas improves the system performance. In this case, the effect of the hardware quality of the AP on the system performance is explored. In Fig. 4.13, the system is observed under

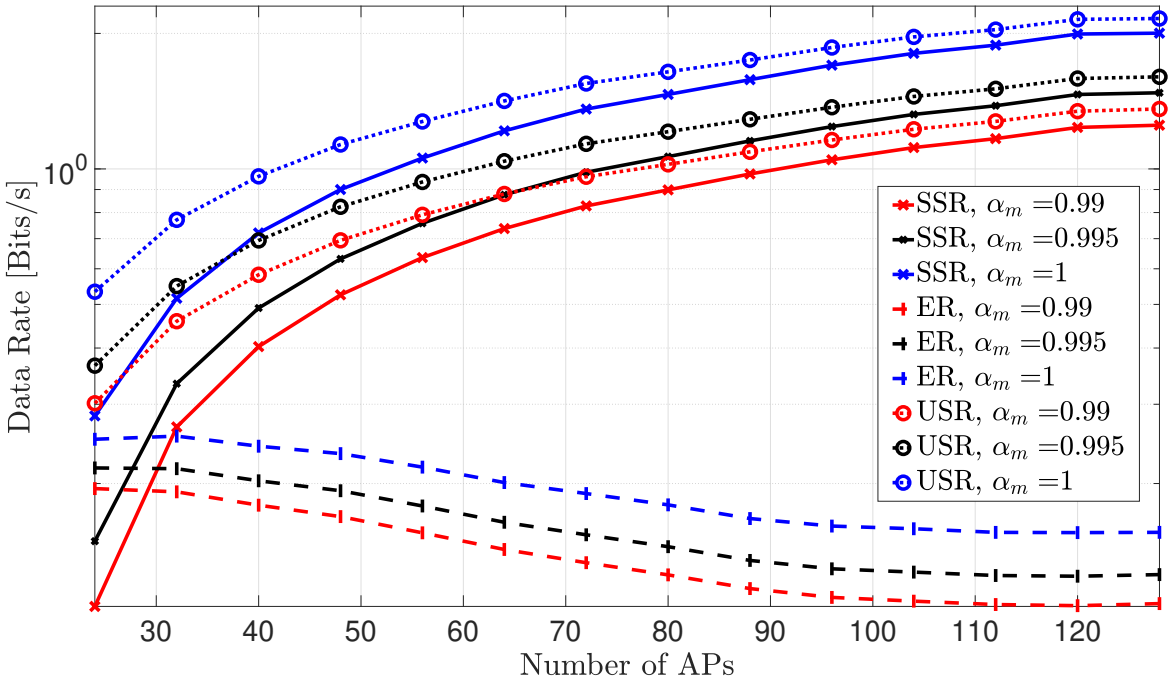

Fig. 4.13 Number of APs Vs. Data Rates with Variable α_m, and $\alpha_e = \alpha_k = 0.995$.

ideal and non-ideal conditions of the hardware quality of the AP, providing insights into the impact of these scenarios on the security and performance of the system. Furthermore, it depicts the USR, ER and SSR under different hardware conditions of the AP, considering $\alpha_m = [0.99, 0.995, 1]$.

To isolate the effect of the hardware quality of the AP, the user and eavesdropper are assumed to have $\alpha_k, \alpha_e = 0.995$, respectively. As the quantity of antennas increases, beamforming is enhanced, improving the SINR_k. Correspondingly, the USR increases due to better signal transmission and reduction in interference, as illustrated in Fig. 4.13. Moreover, the incline in USR is more pronounced under ideal hardware conditions since there is no distortion due to HWIs at the AP.

Observing the ER reveals that as the number of APs grows, less data is intercepted by the eavesdropper. The reason behind this decline is the more effective beamforming of AN towards the null of the users and more efficient beamforming of the users' data streams towards the desired users. Moreover, the decline in ER is more pronounced under non-ideal hardware conditions. This is because, under non-ideal conditions, additional noise and

distortion are introduced by HWIs, leading to a more noticeable decline in ER compared to ideal conditions. Additionally, as the number of AP rises, USR, SSR incline, and ER decline independent of the hardware quality conditions. Furthermore, as the hardware quality of the APs approaches ideal conditions, the amplitude of the ER and USR are greater. Overall, the increase in USR and ER decrease corresponds to an SSR enhancement. Thus, SSR is highest under ideal hardware conditions.

After examining the results presented in Figures 4.11, 4.12, and 4.13, it is evident that increasing the number of APs significantly improves the security and performance of the wireless communication system. The USR consistently increases while the ER decreases. This trend demonstrates a notable enhancement in the SSR, indicating higher transmission of confidential data without eavesdropper interception.

Despite the extensive benefits of increasing the number of APs, the practical implementation involves a considerable cost-quality trade-off. Although increasing the number of APs elevates the security and performance of the system, it also increases infrastructure costs and operational expenses. This trade-off emphasizes the significance of ensuring a balance between security, performance, and economic considerations in increasing the number of APs. Typically, a cost-benefit analysis is performed to determine the optimal number of APs to maximize performance and security while minimizing costs. Implementing network optimization techniques may counteract the economic drawbacks of deploying additional APs in the communication system.

Without the Application of AN

The simulated results demonstrated in the previous sections are generated based on the application of AN. It has been proved that broadcasting AN enhances the security and performance of the system in certain cases. Moreover, without implementing this security measure, the eavesdroppers within the system can retrieve more data. This is evident in Fig. 4.14, in which the ER without AN is shown to be significantly greater than that with AN. At the same time, the users experience enhanced data transmission where there is no AN omission. Subsequently, the USR without omitting AN is greater than the USR with

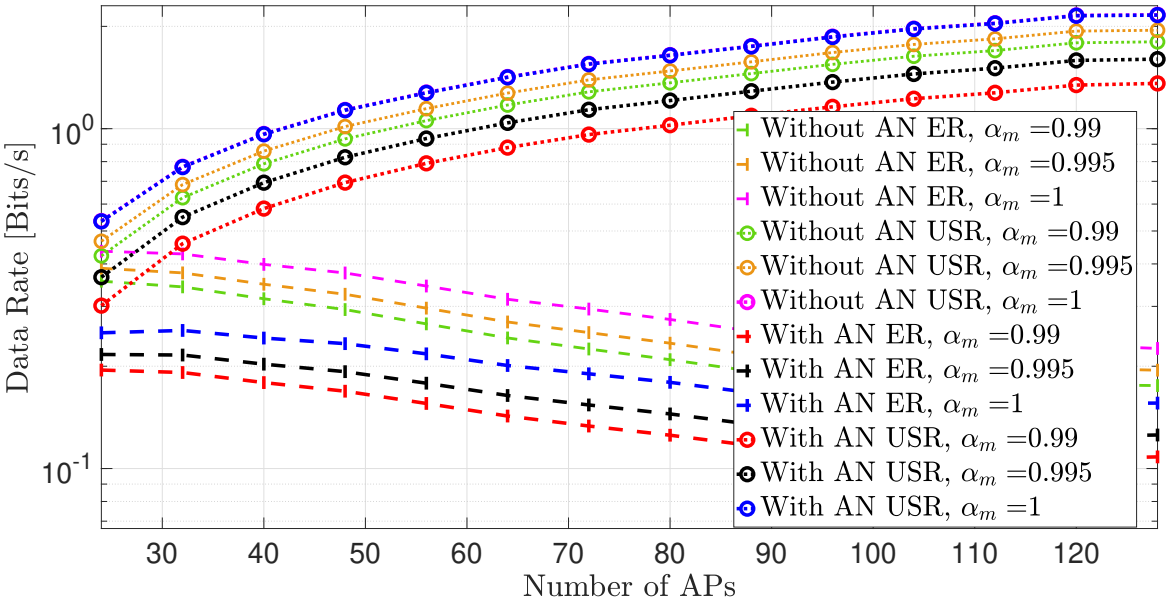

Fig. 4.14 Number of APs Vs. USR and ER given Variable α_m, and $\alpha_e = \alpha_k = 0.995$ with and without AN application.

the application of AN, as depicted in Fig. 4.14. The reason for this lower USR with AN application is described similarly earlier in this thesis. Although the AN is broadcasted from the AP perfectly to the null of the users given perfect CSI, the HWIs generated at the AP due to AN broadcasting degrade the signal at the user end.

In the scenario for which the hardware quality of the AP is ideal, the USR has the highest values. Moreover, in the ideal case, there is an overlap of the USR with AN and without it, indicating that the USR is equivalent regardless of the presence of AN. Additionally, upon observing 4.15 in which the AP has ideal hardware, the SSR with AN broadcasting is greater than the SSR without AN omission.

4.2.3 Assessing the Impact of HWIs as AN Levels Rise

The previous sections demonstrated that increasing transmitted power and the quantity of antennas enhance the performance of the system. Additionally, it was proven that without the presence of AN, the system is vulnerable to eavesdroppers dropping attacks. To improve the security of the system, AN is broadcasted in the null of the users, targeting any eavesdroppers that lie within the network. In prior research [62], [64], it was found that broadcasting AN

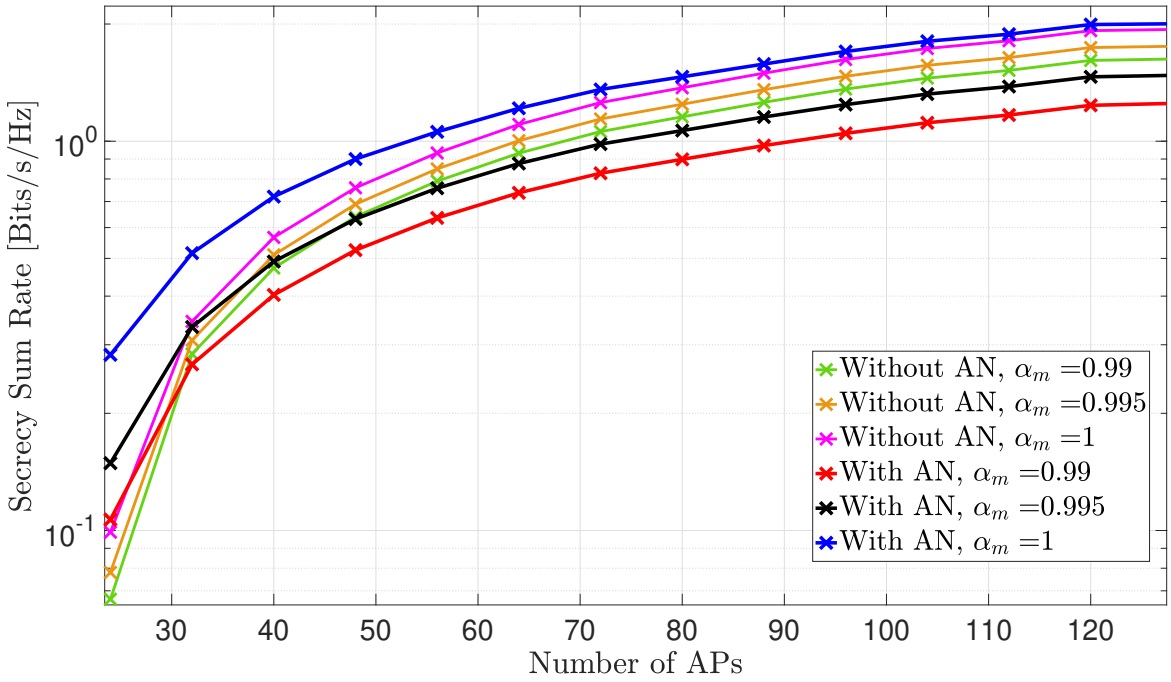

Fig. 4.15 Number of APs Vs. Secrecy Sum Rate given Variable α_m, and $\alpha_e = \alpha_k = 0.995$ with and without AN application.

always enhances the security of the system. However, this observation was established under the assumption that the transceiver is ideal. The focus of this study is to consider hardware imperfections in the transceiver and examine their effect on the security and performance of the system. Furthermore, the impact of increasing AN power levels on the data rates of the user, eavesdropper and AP is investigated. Figures 4.16, 4.17, and 4.18 illustrate variations in USR, ER, and SSR with increasing AN power given defined hardware quality factors. To conduct an in-depth analysis of the impact of HWIs on data rates with increasing AN power, the hardware scaling factors are varied for one communication terminal at a time while assuming the other two terminals to have $\alpha = 0.995$.

Varying User Hardware Quality

For the application of security measures, the hardware quality of the user is a considerable factor that determines the effectiveness of the security as well as the performance of the communication system. Therefore, the quality of the user's hardware is analyzed by varying α_k over the range of values [0.99, 0.995, 1]. For this analysis, the hardware scaling factors of

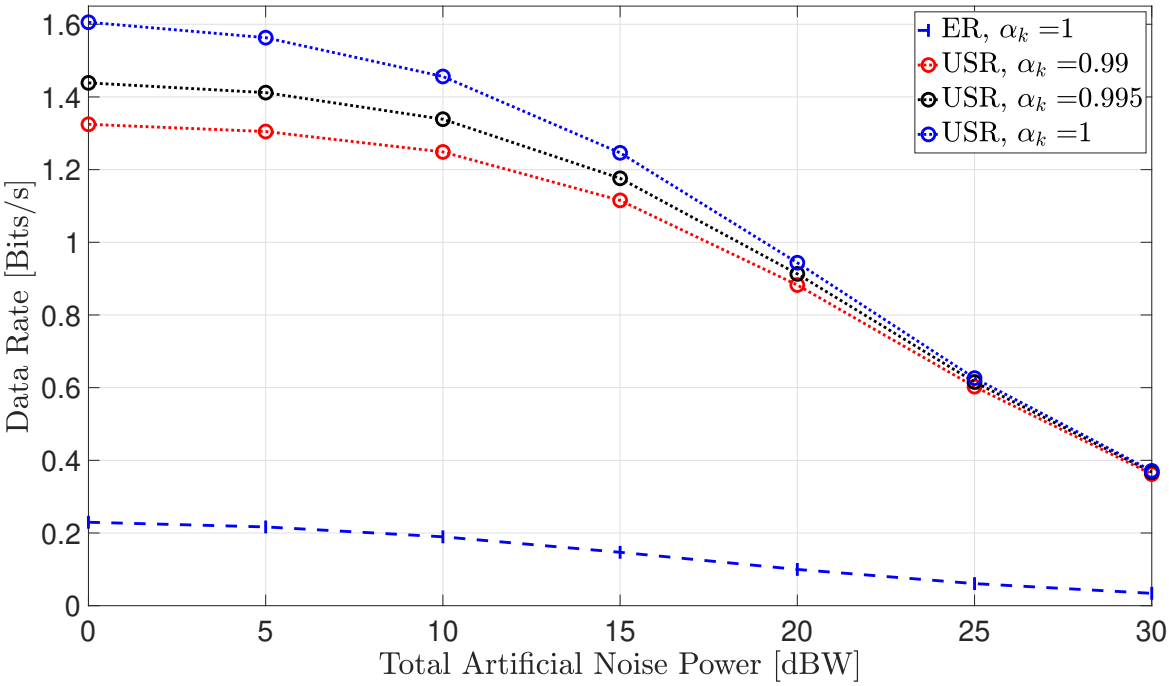

Fig. 4.16 Total AN Power Vs. Data Rates with Variable α_k, and $\alpha_e = \alpha_m = 0.995$.

the eavesdropper and AP is maintained at $\alpha_e, \alpha_m = 0.995$. Moreover, the system is assessed based on the data rates of the user. As evident in Fig. 4.16, the USR declines as the power of the AN increases. This decline in USR is explained by observing the SINR_k equation given in (3.13). It reveals that no terms containing $\bar{p}_d$ are present, however terms associated with P_{rk} and ε_k are dependent on AN (3.12), (3.9). These terms cancel out under ideal hardware conditions, as no distortion associated with HWIs exists in the system. However, when HWIs are present in the system ($\alpha_k = 0.995, 0.99$), P_{rk} and ε_k terms increase as the AN power increases, leading to a decline in SINR_k and consequently the USR.

Varying Eavesdropper Hardware Quality

The analysis conducted thus far emphasizes the detrimental impact of AN broadcasting on the quality of the eavesdropper's signal. This AN power contributes to the distortion of the eavesdropper's signal in two ways. Firstly, it causes jamming noise, negatively impacting the tapped data. Secondly, in the case of imperfect transceiver hardware, it generates HWIs noise.

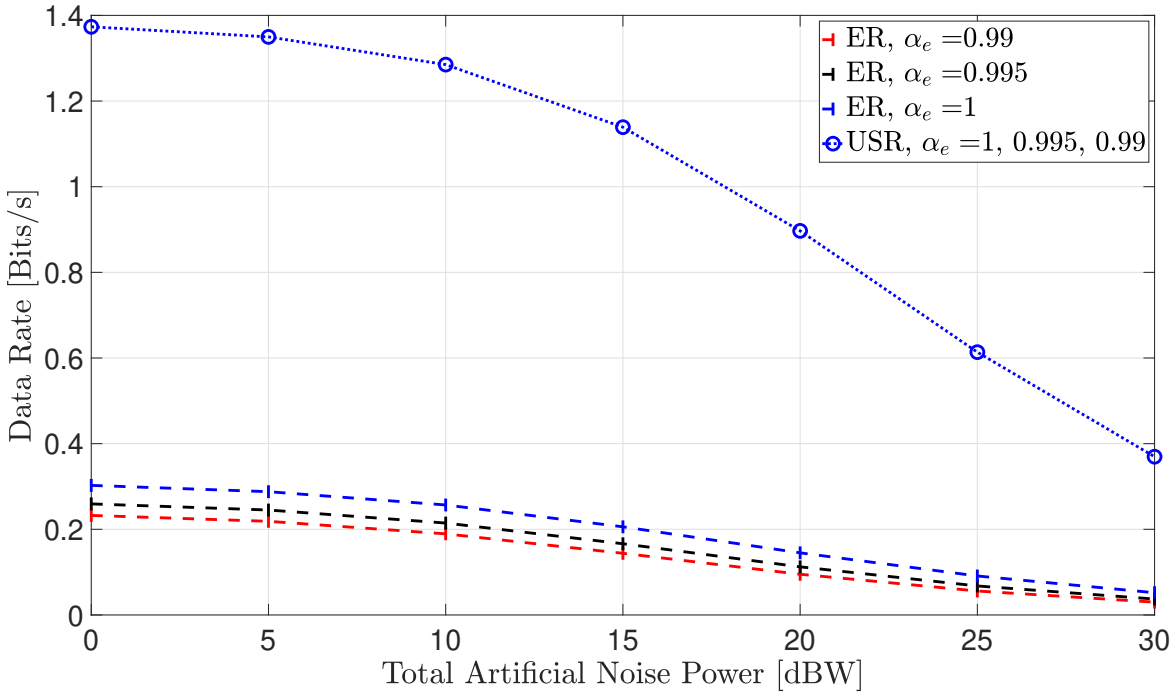

Fig. 4.17 Total AN Power Vs. Data Rates with Variable α_e, and $\alpha_m = \alpha_k = 0.995$.

After examining the ER in Fig. 4.17, it is evident that there is a decrease in the ER with increasing AN levels. Furthermore, this decline in ER is more pronounced as the value of α_e increases. This observation aligns with the examination of SNR_e in (3.17). The equation reveals the existence of the AN term, $\bar{p}_d$, as well as terms dependent on AN including P_{re} and ε_e in (3.16) and (3.8), in its denominator. Under ideal hardware conditions where no distortion associated with HWIs exists, P_{re} and ε_e terms cancel out. However, when HWIs are present in the system ($\alpha_e = 0.995, 0.99$), P_{re} and ε_e terms increase as AN power increases. With this observation and the AN term present in the denominator, there is a decline in SNR_e.

Varying AP Hardware Quality

Unfortunately, in systems featuring imperfect hardware transceivers among legitimate users and APs, the AN broadcasting poses a significant challenge to legitimate user communication. Even when assuming perfect knowledge of users' CSI and precise transmission of AN in the users' null space, this interference detrimentally affects users. This degradation is primarily due to the fact that the AN leads to the generation of increased HWIs noise at the APs.

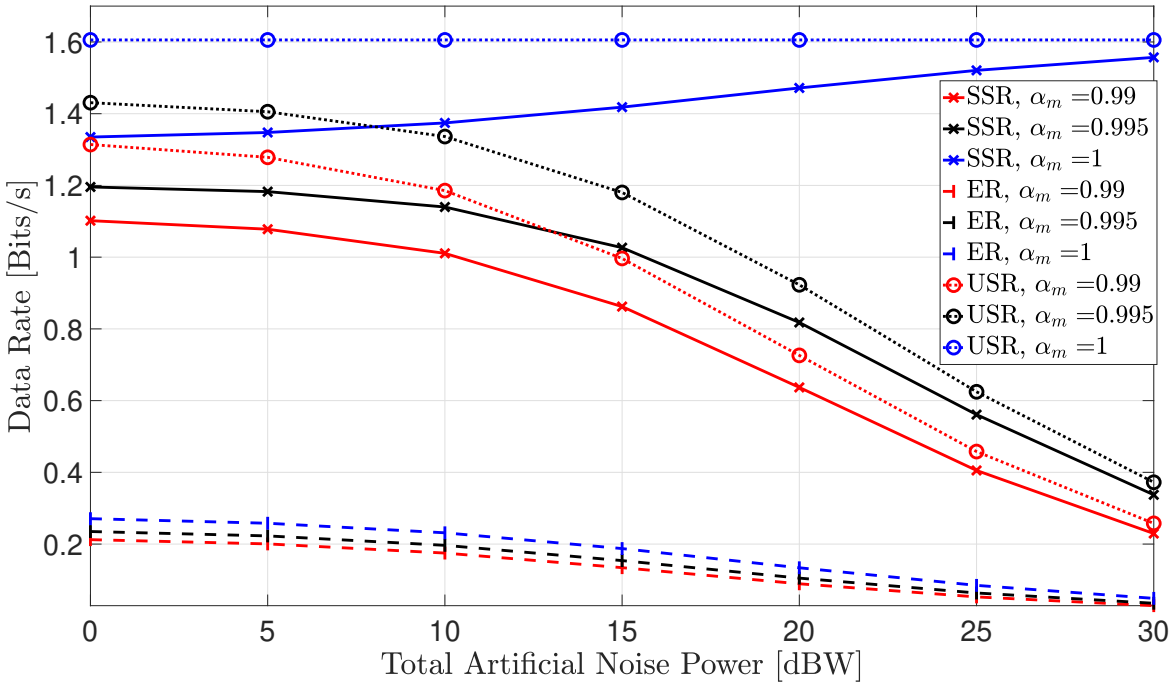

Fig. 4.18 Data Rates Vs. Total AN Power with Variable α_m, and $\alpha_e = \alpha_k = 0.995$.

In the context of Fig. 4.18, the hardware quality of the AP is evaluated. This analysis involves varying the hardware scaling factor of the AP, specifically $\alpha_m = [0.99, 0.995, 1]$, while assuming $\alpha_e, \alpha_k = 0.995$ for the hardware quality of the eavesdroppers and users, respectively. The quality of AP hardware affects both the eavesdropper and legitimate users as evident in the prior analysis of SINR_k and SNR_e.

In the case of ideal AP hardware ($\alpha_m = 1$), it is apparent that the USR is constant regardless of the value of the AN power since there is no HWI distortion at the AP. However in the non ideal scenario, the USR decreases with an increase in AN power. This is due to the degradation caused by AN in the presence of HWIs.

In addition, as the AN power increases, the ER decreases. This decline in ER is attributed to the broadcasting of AN towards the null of the users, which prevents eavesdroppers from tapping confidential data. Moreover, the SSR enhances as AN power increases under the ideal hardware condition of the AP. For the non-ideal scenarios of the APs' hardware, the SSR declines with the increase in AN due to the presence of HWIs. Therefore, incrementing the AN power improves the security of the system in the absence of HWIs at the AP.

This chapter provides an evaluation of the system and security performance of the CF-MaMIMO system. It begins by examining the effect of HWIs under increasing transmitted power, aiming to enhance system performance. Next, it investigates the influence of HWIs when deploying additional APs to further improve system performance. Lastly, it analyzes the impact of HWIs under escalating levels of AN power on the secrecy and perofmance of the system.

Chapter 5

Conclusion and Future Work

5.1 Conclusion

This paper evaluates the application of PLS techniques on the performance of the CF-MaMIMO system. Specifically, it involves beamforming the data streams to the legitimate users and AN to the null of those users. This method protects the system from passive eavesdropping attacks, which compromise the integrity of the confidential data. It has been extensively demonstrated in research that using this security method always enhances the security of the system. However, this observation was only made under the assumption that the transceiver's hardware is ideal.

In practice, equipment used in communication systems, especially in the case of CF-MaMIMO, is expensive due to the large quantity of hardware components. To tackle the issue of system expenses, low-cost hardware components are used, causing the generation of HWIs due to the low quality of these components. Therefore, it is necessary to consider this cost-quality trade-off in practical cases. Moreover, since previous studies have only considered ideal hardware conditions in implementing the security techniques, they neglect the impact of hardware imperfections on the performance and security of the system.

Therefore, this thesis paper examines the impact of HWIs on the PLS of CF-MaMIMO under various hardware quality scenarios for the user, eavesdropper and AP. Each communication terminal's hardware scaling factor is varied to isolate the effect of the hardware quality

of the users, eavesdroppers and APs. Moreover, this thesis explores the impact of increasing AN on data rates for the user and eavesdropper, USR and ER, respectively, and the SSR. It was observed that broadcasting AN to the null of the users degraded the ER and enhanced the SSR for ideal hardware quality conditions of the AP. However, the system performance (USR) declined as AN power levels increased under all hardware conditions.

The transmitted power can be increased to compensate for this decline in system performance. This technique is verified to be highly effective in increasing the USR, according to the illustrations in this thesis. However, increasing the transmitted power increases the ER simultaneously, enabling the eavesdropper to tap more data. Additionally, practicalities in implementation, such as increased energy consumption and elevated noise levels, must be considered when increasing the total transmitted power.

Another method of improving the system performance without increasing the power budget is to deploy more APs. Deploying more AP not only increases the system performance but also decreases the ER and significantly enhances the system's security (SSR). This holds true under all hardware quality scenarios. It was also demonstrated that without the application of AN, the system performance (USR) is higher. The security of the system is highest with AN application under ideal hardware conditions of the APs. Despite the improvement of performance and security of the system, increasing the quantity of APs results in high infrastructure and operational costs. Furthermore, the complexity of the system is significantly increased due to channel estimation and beamforming for the massive amount of APs and the users. The cost-quality trade-off and the computational complexity of the system are drawbacks that need to be considered when deploying more APs.

In conclusion, this work highlights the importance of considering the impact of hardware imperfections on the security and performance of CF-MaMIMO systems. Particularly, it involves implementing PLS techniques including AN beamforming to the null of the users. In addition, this research emphasizes the cost-quality trade-offs of hardware components in infrastructure design. It stands out from previous studies [51], [52], [62], [63], which found that implementing PLS techniques always improves the security of the system. Overall, the

detrimental effects of HWIs on the performance and security of the system necessitate this research.

5.2 Future Works

1. *Power allocation:*

   Improve the security and performance of the communication system, and minimize energy consumption by exploring optimal power allocation algorithms which allocate the transmitted power and AN power levels. Allocating power enables the system to achieve optimal system throughput while mitigating interference and improving spectral efficiency.

2. *Machine Learning:*

   - Enhance received SNR by designing joint user data streams and AN beamforming matrices using machine learning. By utilizing past and real-time data, machine learning can adjust the beamforming weights to maximize the SNR at desired receivers, while nullifying interference from other users and protecting the system from eavesdroppers.
   - Develop machine learning algorithms that allocate the power to enhance the security and performance of the communication system. These algorithms can optimize power allocation by observing system conditions to strengthen the user signal quality and secure the system from unauthorized users.

3. *Channel Estimation:*

   Study PLS techniques under different hardware conditions considering imperfect CSI and pilot contamination. This research considered perfect CSI of the users' channel to ensure effective beamforming of AN to the null of the users. However, in practice, the users' channel is imperfect, requiring channel estimation.

References

[1] International Telecommunication Union. https://www.itu.int/en/Pages/default.aspx, 2025. Accessed: March 18, 2024.

[2] Cybersecurity Ventures. Cybercrime damage costs predicted to reach $10.5 trillion annually by 2025. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/, 2025. Accessed: March 18, 2024.

[3] Marwen Zorgui. *Wireless Physical Layer Security: On the Performance Limit of Secret-Key Agreement*. PhD thesis, 2015.

[4] Matthew Campagna, Lidong Chen, Ozgür Dagdelen, Jintai Ding, J Fernick, Nicolas Gisin, Donald Hayford, Thomas Jennewein, Norbert Lütkenhaus, Michele Mosca, et al. Quantum safe cryptography and security: An introduction, benefits, enablers and challenges. *European Telecommunications Standards Institute*, 8:1–64, 2015.

[5] Rafael F. Schaefer, Gayan Amarasuriya, and H. Vincent Poor. Physical layer security in massive mimo systems. In *2017 51st Asilomar Conference on Signals, Systems, and Computers*, pages 3–8, 2017.

[6] Yulong Zou, Jia Zhu, Xianbin Wang, and Lajos Hanzo. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, 104(9):1727–1765, 2016.

[7] Hao Li. Physical-layer security enhancement in wireless communication systems. 2013.

[8] Abraham Sanenga, Galefang Allycan Mapunda, Tshepiso Merapelo Ludo Jacob, Leatile Marata, Bokamoso Basutli, and Joseph Monamati Chuma. An overview of key technologies in physical layer security. *Entropy*, 22(11):1261, 2020.

[9] Murtaza Ahmed Siddiqi, Heejung Yu, and Jingon Joung. 5g ultra-reliable low-latency communication implementation challenges and operational issues with iot devices. *Electronics*, 8(9):981, 2019.

[10] Aaron D Wyner. The wire-tap channel. *Bell system technical journal*, 54(8):1355–1387, 1975.

[11] Roberto Vera. *A master's thesis*. PhD thesis, University of Applied Sciences, 2010.

[12] Kun Wang, Li Yuan, Toshiaki Miyazaki, Deze Zeng, Song Guo, and Yanfei Sun. Strategic antieavesdropping game for physical layer security in wireless cooperative networks. *IEEE Transactions on Vehicular Technology*, 66(10):9448–9457, 2017.

[13] Matthieu Bloch and Joao Barros. *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[14] Diponkor Bala, GM Waliullah, M Hena, M Abdullah, and M Hossain. Study the performance of capacity for siso, simo, miso and mimo in wireless communication. *Journal of Network and Information Security*, 8(1&2):01–06, 2020.

[15] IEEE Future Networks. Massive mimo, n.d.

[16] Bernard Marr. 2024 iot and smart device trends: What you need to know for the future, October 19 2023.

[17] Erik G Larsson, Ove Edfors, Fredrik Tufvesson, and Thomas L Marzetta. Massive mimo for next generation wireless systems. *IEEE communications magazine*, 52(2):186–195, 2014.

[18] Emil Björnson, Erik G Larsson, and Thomas L Marzetta. Massive mimo: Ten myths and one critical question. *IEEE Communications Magazine*, 54(2):114–123, 2016.

[19] Trinh Van Chien and Emil Björnson. 5g mobile communications. *Cham, Switzerland: 2017. Massive MIMO Communications*, pages 77–116, 2017.

[20] Thomas L Marzetta. Noncooperative cellular wireless with unlimited numbers of base station antennas. *IEEE transactions on wireless communications*, 9(11):3590–3600, 2010.

[21] Jakob Hoydis, Stephan Ten Brink, and Mérouane Debbah. Massive mimo in the ul/dl of cellular networks: How many antennas do we need? *IEEE Journal on selected Areas in Communications*, 31(2):160–171, 2013.

[22] M Nguyen. Massive mimo: a survey of benefits and challenges. *ICSES Trans. Comput. Hardw. Electr. Eng*, 4:1–4, 2018.

[23] Petar Popovski, Čedomir Stefanović, Jimmy J Nielsen, Elisabeth De Carvalho, Marko Angjelichinoski, Kasper F Trillingsgaard, and Alexandru-Sabin Bana. Wireless access in ultra-reliable low-latency communication (urllc). *IEEE Transactions on Communications*, 67(8):5783–5801, 2019.

[24] Jakob Hoydis, Kianoush Hosseini, Stephan Ten Brink, and Mérouane Debbah. Making smart use of excess antennas: Massive mimo, small cells, and tdd. *Bell Labs Technical Journal*, 18(2):5–21, 2013.

[25] Michel Matalatala, Margot Deruyck, Emmeric Tanghe, Luc Martens, Wout Joseph, et al. Optimal low-power design of a multicell multiuser massive mimo system at 3.7 ghz for 5g wireless networks. *Wireless Communications and Mobile Computing*, 2018, 2018.

[26] Hien Quoc Ngo, Alexei Ashikhmin, Hong Yang, Erik G Larsson, and Thomas L Marzetta. Cell-free massive mimo versus small cells. *IEEE Transactions on Wireless Communications*, 16(3):1834–1850, 2017.

[27] Jiakang Zheng, Jiayi Zhang, Hongyang Du, Dusit Niyato, Bo Ai, Mérouane Debbah, and Khaled B Letaief. Mobile cell-free massive mimo: Challenges, solutions, and future directions. *IEEE Wireless Communications*, 2024.

[28] Evizal Abdul Kadir, Raed Shubair, Sharul abdul rahim, M. Himdi, Muhammad Kamarudin, and Sri Rosa. B5g and 6g: Next generation wireless communications technologies, demand and challenges. pages 1–6, 07 2021.

[29] Robin Chataut and Robert Akl. Massive mimo systems for 5g and beyond networks—overview, recent trends, challenges, and future research direction. *Sensors*, 20(10):2753, 2020.

[30] Christoph Studer, Markus Wenk, and Andreas Burg. Mimo transmission with residual transmit-rf impairments. In *2010 international ITG workshop on smart antennas (WSA)*, pages 189–196. IEEE, 2010.

[31] Mohammad Hossein Moghaddam. *Statistical Analysis of Hardware Impairments in Communications Systems*. Chalmers University of Technology, 2023.

[32] Ulf Gustavsson, Cesar Sanchéz-Perez, Thomas Eriksson, Fredrik Athley, Giuseppe Durisi, Per Landin, Katharina Hausmair, Christian Fager, and Lars Svensson. On the impact of hardware impairments on massive mimo. In *2014 IEEE Globecom Workshops (GC Wkshps)*, pages 294–300. IEEE, 2014.

[33] Seyed Aidin Bassam, Mohamed Helaoui, and Fadhel M Ghannouchi. Crossover digital predistorter for the compensation of crosstalk and nonlinearity in mimo transmitters. *IEEE transactions on microwave theory and techniques*, 57(5):1119–1128, 2009.

[34] Steffen Bittner, Andreas Frotzscher, Gerhard Fettweis, and Ellie Deng. Oscillator phase noise compensation using kalman tracking. In *2009 IEEE International Conference on Acoustics, Speech and Signal Processing*, pages 2529–2532. IEEE, 2009.

[35] Emil Björnson, Jakob Hoydis, Marios Kountouris, and Merouane Debbah. Massive mimo systems with non-ideal hardware: Energy efficiency, estimation, and capacity limits. *IEEE Transactions on information theory*, 60(11):7112–7139, 2014.

[36] Chao He and Richard D. Gitlin. System performance of cooperative massive mimo downlink 5g cellular systems. In *2016 IEEE 17th Annual Wireless and Microwave Technology Conference (WAMICON)*, pages 1–5, 2016.

[37] Ashenafi Gebre, Javed Shaikh, Twelegn Kebede, and Fitsum Zerfu Gelete. Comparative performance analysis of channel estimation techniques for massive mimo system. In *2021 IEEE Indian Conference on Antennas and Propagation (InCAP)*, pages 236–239, 2021.

[38] Rongjiang Nie and Li Chen. Performance analysis of massive mimo systems with nonlinear reciprocity mismatch. In *2021 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6, 2021.

[39] Karthik Upadhya, Sergiy A. Vorobyov, and Mikko Vehkapera. Downlink performance of superimposed pilots in massive mimo systems in the presence of pilot contamination. In *2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pages 665–669, 2016.

[40] Idowu Ajayi, Yahia Medjahdi, Rafik Zayani, Lina Mroueh, and Fatima Zohra Kaddour. Papr-aware artificial noise for secure massive mimo downlink. *IEEE Access*, 10:68482–68490, 2022.

[41] Ming Zeng, Nam-Phong Nguyen, Octavia A. Dobre, and H. Vincent Poor. Securing downlink massive mimo-noma networks with artificial noise. *IEEE Journal of Selected Topics in Signal Processing*, 13(3):685–699, 2019.

[42] Wenjin Wang, Xu Chen, Li You, Xinping Yi, and Xiqi Gao. Artificial noise assisted secure massive mimo transmission exploiting statistical csi. *IEEE Communications Letters*, 23(12):2386–2389, 2019.

[43] Tabarek Abood, Ismail Hburi, and Hasan Fahad Khazaal. Massive mimo: An overview, recent challenges, and future research directions. In *2021 International Conference on Advance of Sustainable Engineering and its Application (ICASEA)*, pages 43–48, 2021.

[44] Mohammed A. AlQaisei, Abdel-Fattah A. Sheta, and Ibrahim Elshafiey. Hybrid beamforming for multi-user massive mimo systems at millimeter-wave networks. In *2022 39th National Radio Science Conference (NRSC)*, volume 1, pages 181–187, 2022.

[45] Furqan Jameel, Faisal, M. Asif Ali Haider, and Amir Aziz Butt. Massive mimo: A survey of recent advances, research issues and future directions. In *2017 International Symposium on Recent Advances in Electrical Engineering (RAEE)*, pages 1–6, 2017.

[46] Navneet Garg, Hanxiao Ge, and Tharmalingam Ratnarajah. Generalized superimposed training scheme in irs-assisted cell-free massive mimo systems. *IEEE Journal of Selected Topics in Signal Processing*, 16(5):1157–1171, 2022.

[47] Enyu Shi, Jiayi Zhang, Ruisi He, Huiying Jiao, Zhiqin Wang, Bo Ai, and Derrick Wing Kwan Ng. Spatially correlated reconfigurable intelligent surfaces-aided cell-free massive mimo systems. *IEEE Transactions on Vehicular Technology*, 71(8):9073–9077, 2022.

[48] Seyyed Saleh Hosseini. *Studies in Cell-Free Massive-MIMO: Green Power Allocation, Physical Security, and DoA Estimation*. McGill University (Canada), 2022.

[49] Rafael F Schaefer, Gayan Amarasuriya, and H Vincent Poor. Physical layer security in massive mimo systems. In *2017 51st Asilomar conference on signals, systems, and computers*, pages 3–8. IEEE, 2017.

[50] Kang An, Tao Liang, Xiaojuan Yan, and Gan Zheng. On the secrecy performance of land mobile satellite communication systems. *IEEE Access*, 6:39606–39620, 2018.

[51] Kishan Neupane, Rami J Haddad, and David L Moore. Secrecy analysis of massive mimo systems with mrt precoding using normalization methods. In *SoutheastCon 2018*, pages 1–6. IEEE, 2018.

[52] Tinghan Yang, Rongqing Zhang, Xiang Cheng, and Liuqing Yang. Secure massive mimo under imperfect csi: Performance analysis and channel prediction. *IEEE Transactions on Information Forensics and Security*, 14(6):1610–1623, 2018.

[53] Dzevdan Kapetanovic, Gan Zheng, and Fredrik Rusek. Physical layer security for massive mimo: An overview on passive eavesdropping and active attacks. *IEEE Communications Magazine*, 53(6):21–27, 2015.

[54] Xianyu Zhang, Daoxing Guo, Kefeng Guo, and Hehao Niu. Secure performance analysis and detection of pilot attack in massive multiple-input multiple-output system. *International Journal of Distributed Sensor Networks*, 14(5):1550147718776922, 2018.

[55] Jun Zhu, Robert Schober, and Vijay K Bhargava. Secure transmission in multicell massive mimo systems. *IEEE Transactions on Wireless Communications*, 13(9):4766–4781, 2014.

[56] Yongpeng Wu, Robert Schober, Derrick Wing Kwan Ng, Chengshan Xiao, and Giuseppe Caire. Secure massive mimo transmission with an active eavesdropper. *IEEE Transactions on Information Theory*, 62(7):3880–3900, 2016.

[57] Jun Zhu, Wei Xu, and Ning Wang. Secure massive mimo systems with limited rf chains. *IEEE Transactions on Vehicular Technology*, 66(6):5455–5460, 2016.

[58] Sanghun Im, Hyoungsuk Jeon, Jinho Choi, and Jeongseok Ha. Secret key agreement with large antenna arrays under the pilot contamination attack. *IEEE Transactions on Wireless Communications*, 14(12):6579–6594, 2015.

[59] Y Ozan Basciftci, C Emre Koksal, and Alexei Ashikhmin. Securing massive mimo at the physical layer. In *2015 IEEE Conference on Communications and Network Security (CNS)*, pages 272–280. IEEE, 2015.

[60] Kaifeng Guo, Yan Guo, and Gerd Ascheid. Security-constrained power allocation in mu-massive-mimo with distributed antennas. *IEEE Transactions on Wireless Communications*, 15(12):8139–8153, 2016.

[61] Xianyu Zhang, Daoxing Guo, Kang An, Wenfeng Ma, and Kefeng Guo. Secure transmission and power allocation in multiuser distributed massive mimo systems. *Wireless Networks*, 26(2):941–954, 2020.

[62] Jun Zhu, Robert Schober, and Vijay K Bhargava. Linear precoding of data and artificial noise in secure massive mimo systems. *IEEE Transactions on Wireless Communications*, 15(3):2245–2261, 2015.

[63] Dhanushka Kudathanthirige, Santosh Timilsina, and Gayan Amarasuriya Aruma Baduge. Secure communication in relay-assisted massive mimo downlink with active pilot attacks. *IEEE Transactions on Information Forensics and Security*, 14(11):2819–2833, 2019.

[64] Satashu Goel and Rohit Negi. Guaranteeing secrecy using artificial noise. *IEEE transactions on wireless communications*, 7(6):2180–2189, 2008.

[65] Jue Wang, Jemin Lee, Fanggang Wang, and Tony QS Quek. Jamming-aided secure communication in massive mimo rician channels. *IEEE Transactions on Wireless Communications*, 14(12):6854–6868, 2015.

[66] Xiaoming Chen, Lei Lei, Huazi Zhang, and Chau Yuen. Large-scale mimo relaying techniques for physical layer security: Af or df? *IEEE Transactions on Wireless Communications*, 14(9):5135–5146, 2015.

[67] Tiep M Hoang, Hien Quoc Ngo, Trung Q Duong, Hoang Duong Tuan, and Alan Marshall. Cell-free massive mimo networks: Optimal power control against active eavesdropping. *IEEE Transactions on Communications*, 66(10):4724–4737, 2018.

[68] Anastasios K Papazafeiropoulos, Emil Björnson, Pandelis Kourtessis, Symeon Chatzinotas, and John M Senior. Scalable cell-free massive mimo systems with hardware impairments. In *2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*, pages 1–7. IEEE, 2020.

[69] Tim Schenk. *RF imperfections in high-rate wireless systems: impact and digital compensation*. Springer Science & Business Media, 2008.

[70] Rajet Krishnan, Mohammad Reza Khanzadi, N Krishnan, Yongpeng Wu, Alexandre Graell i Amat, Thomas Eriksson, and Robert Schober. Linear massive mimo precoders in the presence of phase noise—a large-scale analysis. *IEEE Transactions on Vehicular Technology*, 65(5):3057–3071, 2015.

[71] Jun Zhu, Ning Wang, and Vijay K Bhargava. Per-antenna constant envelope precoding for secure transmission in large-scale miso systems. In *2015 IEEE/CIC International Conference on Communications in China (ICCC)*, pages 1–6. IEEE, 2015.

[72] Hardware Scaling Laws. Massive mimo with non-ideal arbitrary arrays: Hardware scaling laws and circuit-aware design. 2015.

[73] Xiangyun Zhou and Matthew R McKay. Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation. *IEEE Transactions on Vehicular Technology*, 59(8):3831–3842, 2010.

[74] Jun Zhu, Derrick Wing Kwan Ng, Ning Wang, Robert Schober, and Vijay K Bhargava. Analysis and design of secure massive mimo systems in the presence of hardware impairments. *IEEE Transactions on Wireless Communications*, 16(3):2001–2016, 2017.

[75] Jun Zhu, Ye Li, Ning Wang, and Wei Xu. Wireless information and power transfer in secure massive mimo downlink with phase noise. *IEEE Wireless Communications Letters*, 6(3):298–301, 2017.

[76] Jiayi Zhang, Yinghua Wei, Emil Björnson, Yu Han, and Shi Jin. Performance analysis and power control of cell-free massive mimo systems with hardware impairments. *IEEE Access*, 6:55302–55314, 2018.

[77] Hamed Masoumi and Mohammad Javad Emadi. Performance analysis of cell-free massive mimo system with limited fronthaul capacity and hardware impairments. *IEEE Transactions on Wireless Communications*, 19(2):1038–1053, 2019.

[78] Xiaoling Hu, Caijun Zhong, Xiaoming Chen, Weiqiang Xu, Hai Lin, and Zhaoyang Zhang. Cell-free massive mimo systems with low resolution adcs. *IEEE Transactions on Communications*, 67(10):6844–6857, 2019.

[79] Jiakang Zheng, Jiayi Zhang, Luming Zhang, Xiaodan Zhang, and Bo Ai. Efficient receiver design for uplink cell-free massive mimo with hardware impairments. *IEEE Transactions on Vehicular Technology*, 69(4):4537–4541, 2020.

[80] Xianyu Zhang, Daoxing Guo, Kang An, and Bangning Zhang. Secure communications over cell-free massive mimo networks with hardware impairments. *IEEE Systems Journal*, 14(2):1909–1920, 2019.

[81] Emil Björnson, Jakob Hoydis, Luca Sanguinetti, et al. Massive mimo networks: Spectral, energy, and hardware efficiency. *Foundations and Trends® in Signal Processing*, 11(3-4):154–655, 2017.

[82] Elina Nayebi, Alexei Ashikhmin, Thomas L Marzetta, Hong Yang, and Bhaskar D Rao. Precoding and power optimization in cell-free massive mimo systems. *IEEE Transactions on Wireless Communications*, 16(7):4445–4459, 2017.