SECURE BEAMFORMING FOR MILLIMETER WAVE COMMUNICATIONS

A Thesis Submitted to
the Graduate School of
İzmir Institute of Technology
in Partial Fulfillment of the Requirements for the Degree of

MASTER OF SCIENCE

in Electronics and Communication Engineering

by
Oğulcan ERDOĞAN

July 2020
İZMİR

ACKNOWLEDGMENTS

I would like to express my gratitude to my supervisor Assoc. Prof. Dr. Berna ÖZBEK for her guidance, support, and motivation during this thesis.

I would also like to express my gratitude to my committee members Assoc. Prof. Dr. Mustafa Aziz ALTINKAYA and Assoc. Prof. Dr. Ahmet ÖZKURT for their contributions and valuable advices.

Izmir Institute of Technology deserves my gratitude for its excellent education programs and research experiences. I owe everything to them what I learned so far.

Finally, I would like to thank my whole family for their endless love, support and patience. Without them, I would not succeed.

Last but not least, I am also grateful to my colleagues. Special thanks to Ceren ÖZKAL, Anıl KARATAY, Bilal Orkan OLCAY, and Mert İLGÜY for their help and valuable support.

ABSTRACT

SECURE BEAMFORMING FOR MILLIMETER WAVE COMMUNICATIONS

Over the last decade, many advancements have been made in the field of wireless communications. Among the major technology enablers being explored for the fifth-generation (5G) networks at the physical layer (PHY), a great deal of attention has been focused on millimeter-wave (mmWave) communications, massive multiple-input multiple-output (MIMO) antenna systems and beamforming techniques. These enablers bring to the forefront great opportunities for enhancing the performance of 5G and beyond-5G networks, concerning throughput, spectral efficiency, energy efficiency, latency, and reliability.

At the meantime, the wireless communication is prone to information leakage to the unintended nodes due to its open nature. Hence, the secure communication is becoming more critical in the wireless networks. To address this challenge, the concept of Physical Layer Security (PLS) is explored. In this thesis, we examine the statistical mmWave transmission through linear beamforming techniques for PLS based systems. We propose the secure multiuser (MU) MIMO mmWave communications by employing hybrid beamforming at the base stations (BS), legitimate users and eavesdroppers. Using a 3 Dimensional mmWave channel model for each node, we employ the artificial noise (AN) beamforming to jam the channels of eavesdroppers and to enhance the secrecy capacity of the overall communication system. We investigate the secrecy performance on different scenarios including the single cell and multicell mmWave MU-MIMO downlink communications and reveal the key points directly related to the system security.

ÖZET

MİLİMETRE DALGA İLETİŞİM İÇİN GÜVENLİ HÜZME OLUŞTURMA

Son on yılda kablosuz iletişim alanında birçok gelişme sağlanmıştır. Fiziksel katmandaki beşinci nesil (5N) ağlar için araştırılan önemli teknoloji sağlayıcıları arasında, milimetre dalga iletişimine, çok girişli çok çıkışlı (ÇGÇÇ) çok sayıdaki anten sistemlerine ve ışın hüzmelendirme tekniklerine büyük bir ilgi gösterilmektedir. 5N'ye yön veren bu teknolojiler, spektral verimlilik, enerji verimliliği, gecikme ve güvenilirlik açısından 5N ve 5N'nin ötesindeki ağların performansını artırmak için büyük fırsatlara sahiptir.

Aynı zamanda kablosuz iletişim, açık doğası nedeniyle gizli dinleyicilere bilgi sızıntısına eğilimlidir. Bu nedenle, kablosuz ağlarda güvenli iletişim daha kritik hale gelmektedir. Bu sorunu çözmek için, Fiziksel Katman Güvenliği (FKG) kavramı araştırılmaktadır. Bu tezde FKG tabanlı sistemler için doğrusal ışın şekillendirme teknikleri ile istatistiksel milimetre dalga iletimini inceliyoruz. Baz istasyonunda, meşru kullanıcılarda ve gizli dinleyicilerde hibrid ışın hüzmelendirme kullanarak güvenli çok kullanıcılı ÇGÇÇ milimetre dalga iletişimlerini öneriyoruz. Her bir gönderici ve alıcı çifti için 3 boyutlu milimetre dalga kanal modeli kullanarak, gizli dinleyicilerin kanallarını bastırmak ve genel iletişim sisteminin gizlilik kapasitesini arttırmak için yapay gürültü ışın hüzmelendirme kullanıyoruz. Tek hücreli ve çok hücreli milimetre dalga ÇGÇÇ uydu-yer hattı iletişimi de dahil olmak üzere farklı senaryolardaki gizlilik performansını araştırıyoruz ve doğrudan sistem güvenliği ile ilgili kilit noktaları ortaya çıkarıyoruz.

TABLE OF CONTENTS

LIST OF FIGURES

Figure **Page**

Figure **Page**

LIST OF TABLES

Table **Page**

LIST OF ABBREVIATIONS

3GPP . . . . . 3rd Generation Partnership Project
5G . . . . . 5th Generation
AoA . . . . . Angle of Arrival
AoD . . . . . Angle of Departure
BS . . . . . Base Station
CoMP . . . . . Coordinated Multi-Point Transmission/Reception
CSI . . . . . Channel State Information
CSIT . . . . . Channel State Information at Transmitter
LoS . . . . . Line of Sight
MF . . . . . Matched Filter
MIMO . . . . . Multiple Input Multiple Output
MMSE . . . . . Minimum Mean Square Error
mmWave . . . . . Millimeter Wave
MRC . . . . . Maximum Ratio Combining
MRT . . . . . Maximum Ratio Transmission
MU . . . . . Multi User
nLoS . . . . . non-Line of Sight
non-CoMP . . . . . non-Coordinated Multi-Point Transmission/Reception
PHY . . . . . Physical Layer
PLS . . . . . Physical Layer Security
RF . . . . . Radio Frequency
SCM . . . . . Spatial Channel Model
SINR . . . . . Signal to Interference plus Noise Ratio
SNR . . . . . Signal to Noise Ratio
SSCM . . . . . Statistical Spatial Channel Model
SU . . . . . Single User
SVD . . . . . Singular Value Decomposition
ULA . . . . . Uniform Linear Array
UPA . . . . . Uniform Planar Array
ZF . . . . . Zero Forcing

CHAPTER 1

INTRODUCTION

Nowadays, wireless networks have been becoming much attractive research topics more than ever. Bringing new challenges and opportunities, the next-generation communication is a critical advancement in the center of this idea. Moreover, the key technological enabler of the next-generation communication is the mmWave frequencies which can shift the frequency bands to the mmWave available bands. The mmWave provides ultra-fast communication, low latency and higher data rates (Rappaport et al., 2013). Besides these properties, the mmWave makes also possible to use smaller antennas due to its smaller wavelength. Considering this advantage, the large antenna arrays can be formed to exploit the spatial degree of freedom.

In the MIMO systems, multiple transmitters and receivers can simultaneously communicate each other by forming their signals to the intended direction via 'beamforming' (Alkhateeb et al., 2014). For the mmWave perspective and using large antenna arrays, the narrow beam can be obtained. However, the large antenna arrays consumes much more power than the conventional systems. The hybrid scheme combining the analog and digital beamforming has been presented to ensure the power efficiency on such a large arrays (Ahmed et al., 2018). Thus, the hybrid beamforming is the inevitable part of MIMO systems.

Besides many advantages of mmWave and hybrid MIMO, there are still lots of concerns for the next-generation communication systems. One of these concerns, probably the most important one, is security. While the next-generation communication systems support the massive number of devices connecting them to the virtual world, the conventional cryptographic techniques including key generation and distribution become more and more important and challenging tasks. To address this challenge, the concept of Physical Layer Security (PLS) is being introduced and explored for the wireless communication systems as a complement solution of cryptographic techniques (Khisti and Wornell, 2010a), (Khisti and Wornell, 2010b).

The information theory based PLS approach focuses on the secrecy capacity of the

propagation channels. The aim of PLS is to completely eliminate or reduce somehow the effects of eavesdropping attacks by the unauthorized receivers or transmitters (Wu et al., 2018). In the literature, there are two types of eavesdropping attacks which are called as active and passive. The active eavesdroper behaves as a transmitter and tries to jam the legitimate user's channel. Conversely, the passive eavesdropper wants to hide its presence from the transmitter and tries to obtain any information from the legitimate user's channel. Each type of eavesdropping attack must be carefully examined and properly set a strategy to overcome these attacks. In this thesis, we consider only the passive eavesdropper attacks since the passive eavesdropping is more often in the practical applications.

There are several studies about PLS techniques in the literature for sub-6 GHz systems. The most effective and probably the most common way to enhance the secrecy capacity as well as improve the performance of PLS systems is to use multiple antenna techniques. In addition, the artificially generated noise can be combined with beamforming which is the AN beamforming proposed by (Goel and Negi, 2008) to enhance secrecy capacity with degrading the channel of eavesdroppers. The PLS with beamforming techniques have been extensively studied in the literature (Hong et al., 2013), (Mukherjee et al., 2014), (Yang et al., 2015), (Ju et al., 2017). However, there are limited number of PLS studies for the mmWave MIMO systems.

In this thesis, we examine the PLS with hybrid beamforming techniques for the mmWave MIMO systems. We focus on the mmWave multiuser MIMO communications with multiple streams for both the single cell and multicell scenarios by considering the hybrid scheme at both the transmitter and receiver side for making practical and a realizable scenario. We propose PLS scenarios including AN beamforming in the mmWave multiuser MIMO systems. Moreover, we present comprehensive studies about different linear beamforming techniques including maximum ratio transmission (MRT), zero-forcing (ZF), minimum mean square error (MMSE).

The rest of this thesis is organized as follows:

- Chapter 2 describes the mmWave channel models, massive MIMO concept with hybrid beamforming techniques. The performance evaluations are provided for different number of users and antennas in the single cell scenario.

- Chapter 3 presents the secure mmWave multiuser MIMO communication in the single cell case. Considering multiple antennas at both ends and multiple streams

for the multiple users, the MMSE beamforming combining with AN is investigated. The simulation results for the PLS in single cell using MMSE and AN beamforming are given.

- In Chapter 4, the PLS is applied to the multicell mmWave multiuser MIMO communication system. Both the performance of coordinated and non-coordinated linear beamforming techniques are examined on the system security. The impact of complexity and reliability are presented for the linear beamforming techniques. The simulation results are provided for multicell mmWave communication system using AN beamforming.

- Finally, Chapter 5 gives the conclusion and summarizes the future directions.

CHAPTER 2

MILLIMETER-WAVE MULTIUSER MIMO SYSTEMS

This chapter examines the main technological enablers for the next-generation wireless communication systems. One of these is the mmWave spectrum that provides small wavelength via high frequency range (from 30GHz to 300GHz) (Hemadeh et al., 2017). In addition to this, the massive MIMO is one of the most promising technology (Swindlehurst et al., 2014). The mmWave spectrum supports the large number of antennas for both BSs and user sides. It provides a great number of degree of freedom on the mmWave communication systems with beamforming techniques.

In this chapter, firstly, the mmWave channel model is given. Then, the massive MIMO systems with hybrid beamforming techniques are provided. Finally, the simulation results are given for both the single user (SU) MIMO and multiuser (MU) MIMO communications.

2.1. mmWave Channel Modeling

Developing a channel model is essential for both understanding and analyzing the real world behaviour of any frequency spectrum. Until now, the channel modeling of sub-6GHz and mmWave bands that are already used in a diverse range of communication systems have allowed us to examine their physical characteristics to construct the new theories as well as the new technologies.

The stochastic channel modeling is considered more suitable for the simulation and design purposes. The Saleh-Valenzuela model and the 3rd Generation Partnership Project (3GPP) Spatial Channel Model (SCM) are two examples of the most commonly used stochastic channel models (Hemadeh et al., 2017).

Based on the 3GPP SCM, a three-dimensional (3D) statistical spatial channel model (SSCM) for the mmWave MIMO system has been considered (Samimi and Rappaport, 2016). Since the mmWave channel is known as sparse channel where the propagation tends to be *line-of-sight* (LoS), there are only limited number of resolvable paths

including LoS and highly correlated *non-line-of-sight* (nLoS). Another reason for this is the strong attenuation since the mmWave frequencies are more vulnerable to high path loss compared to the sub-6GHz frequencies (Swindlehurst et al., 2014). From the LoS dominant point of view, the mmWave channel model is defined by (Hemadeh et al., 2017),

$$\mathbf{H} = \mathbf{H}_{LoS} + \mathbf{H}_{nLoS} \tag{2.1}$$

where $\mathbf{H}_{LoS}$ denotes the LoS component of the mmWave channel which is given as,

$$\mathbf{H}_{LoS} = \alpha_{LoS} \cdot \mathbf{a}(\varphi_{LoS}^{Rx}, \theta_{LoS}^{Rx}) \cdot \mathbf{a}^{H}(\varphi_{LoS}^{Tx}, \theta_{LoS}^{Tx}) \tag{2.2}$$

Another component of the mmWave channel in Eq.(2.1) is the nLoS component, $\mathbf{H}_{nLoS}$, is defined as,

$$\mathbf{H}_{nLoS} = \frac{1}{\sqrt{S_c}} \sum_{c=1}^{C} \sum_{s=1}^{S_c} \alpha_{c,s} \cdot \mathbf{a}(\varphi_{c,s}^{Rx}, \theta_{c,s}^{Rx}) \cdot \mathbf{a}^{H}(\varphi_{c,s}^{Tx}, \theta_{c,s}^{Tx}) \tag{2.3}$$

where C and S_c denotes the number of clusters and the number of subpaths in each cluster, respectively. The instantaneous complex coefficient of each subpath is represented by α. Moreover, φ and θ indicate the azimuth angles and the elevation angles and $\mathbf{a}(\varphi, \theta)$ denotes angle of arrival (AoA) or angle of departure (AoD) array response which correspond to the receiver and the transmitter, respectively (Hemadeh et al., 2017).

The probability of a link being in LoS condition is given by (Samimi and Rappaport, 2016),

$$P_{\text{LoS}}(d) = \left[\min\left(\frac{27}{d}, 1\right)\left(1 - e^{-\frac{d}{71}}\right) + e^{-\frac{d}{71}}\right]^2 \tag{2.4}$$

where d is the distance between the transmitter and receiver. In this case, if the distance between the transmitter and receiver is less than 27 meters, LoS definitely occurs except that there is no blockage in the environment.

In the MIMO system, both the uniform linear array (ULA) and the uniform planar array (UPA) configuration can be used by considering array factor $\mathbf{a}(\varphi, \theta)$. Although the ULA is simpler and more practical, the UPA must be taken into account for the large scale antenna arrays especially square and rectangular ones. For the ULA, the antenna array response is defined by (Hemadeh et al., 2017),

$$\mathbf{a}(\varphi) = \frac{1}{\sqrt{M}}[1, \ldots, e^{j(m-1)\frac{2\pi}{\lambda}d_x \sin(\varphi)}, \ldots, e^{j(M-1)\frac{2\pi}{\lambda}d_x \sin(\varphi)}]^T \tag{2.5}$$

where M is the number of antennas in horizontal axis and λ is the wavelength ($\lambda = c/f$). The inter-element spacing (distance between two adjacent antenna elements) is indicated by d_x. For the UPA, the antenna array response is given by (Hemadeh et al., 2017),

$$\mathbf{a}(\varphi, \theta) = \frac{1}{\sqrt{MN}}[1 \ldots, e^{j[(m-1)\Psi_1 + (n-1)\Psi_2]}, \ldots, e^{j[(M-1)\Psi_1 + (N-1)\Psi_2]}]^T \tag{2.6}$$

where Ψ_1 and Ψ_2 are defined as,

$$\begin{aligned} \Psi_1 &= \frac{2\pi}{\lambda} d_x \cos(\varphi) \sin(\theta) \\ \Psi_2 &= \frac{2\pi}{\lambda} d_y \sin(\varphi) \sin(\theta) \end{aligned} \tag{2.7}$$

where M and N are the number of antennas in the horizontal axis and in vertical axis, respectively. The inter-element spacing between two adjacent antenna elements for both the horizontal axis and vertical axis are indicated by d_x and d_y, respectively.

2.2. Massive MIMO and Hybrid Architecture

On one hand, the MIMO exploit the diversity of antennas which provides the spectral efficiency enhancement on the system performance (Molisch et al., 2017) (Ahmed et al., 2018). On the other hand, the mmWave spectrum makes possible to construct the large antenna arrays due to its small wavelengths. Moreover, the massive-MIMO

that consists of tens of ordered antennas has emerged by the mmWave for both BSs and users (Swindlehurst et al., 2014). The main advantage of the massive-MIMO is to provide highly directional radio propagation. It also supports simple linear signal processing techniques such as MRT or maximum ratio combining (MRC) with significant performance improvement (Swindlehurst et al., 2014) (Ahmed et al., 2018).

The massive-MIMO brings its benefits and costs along. While increasing antennas and RF chains has led the degree of freedom for serving large number of users with increasing the data streams, they consumes much more power as directly related to the number of active users and the streams. To overcome this problem and enhance the power and energy efficiency, the hybrid scheme was given in (El Ayach et al., 2014). In the hybrid scheme, the number of antennas remains same whereas the number of RF chains is decreased. In this way, both the degree of freedom for the signal processing techniques and the power efficiency are provided (El Ayach et al., 2014).

The hybrid scheme consists of the two parts that are the analog and digital shown in Figure (2.1). The first part is the analog part that is composed of phase shifters that are cheaper and consume less power than RF chains. An RF chain is composed of RF components such as ADC/DAC, filters, mixers, etc. Therefore, especially in the high-frequency domain, using more RF chains consume much power compared to the phase shifters (El Ayach et al., 2014) (Sun et al., 2018). The second part is the digital part that is responsible for operating the signal processing techniques shown in Figure (2.1).

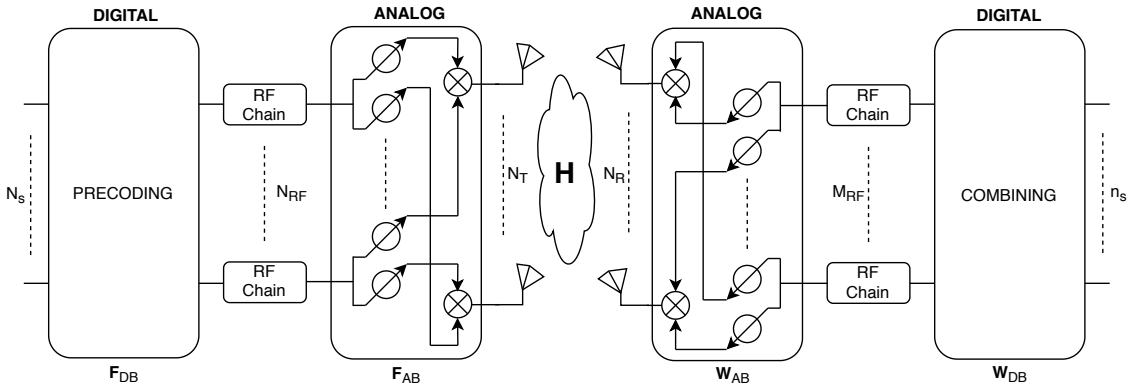

Figure 2.1. Hybrid beamforming for single user mmWave communication.

In Figure (2.1), the transmitter has N_T antennas and the receiver has N_R antennas.

N_s and n_s are defined as the number of data stream at transmitter and receiver, respectively. N_{RF} and M_{RF} are denoted as the number of RF chains at the transmitter and receiver, respectively. While $\mathbf{F}$ indicates the precoding matrix at the transmitter side, $\mathbf{W}$ is the combining matrix at the receiver side. Because of the hybrid scheme, $\mathbf{F}_{DB}$ or $\mathbf{W}_{DB}$ and $\mathbf{F}_{AB}$ or $\mathbf{W}_{AB}$ are denoted as the digital beamformer and the analog beamformer, respectively. The lower indices are used to separate these two beamformers as the digital or analog. On one hand, the digital beamformer $\mathbf{F}_{DB}$ and $\mathbf{W}_{DB}$ have the dimension of $N_{RF} \times N_s$ and $M_{RF} \times n_s$, respectively. On the other hand, the analog beamformers $\mathbf{F}_{AB}$ and $\mathbf{W}_{AB}$ have the dimension of $N_T \times N_{RF}$ and $N_R \times M_{RF}$, respectively. The reliable communication is provided by using hybrid scheme when the system satisfies $N_T \geq N_{RF} \geq N_s$ and $N_R \geq M_{RF} \geq n_s$ constraints.

2.3. System Model for Single Cell Single User Case

Considering a single cell SU-MIMO downlink mmWave communication system, the received signal by the user is expressed as (El Ayach et al., 2014),

$$\mathbf{y} = \sqrt{P}\mathbf{W}_{DB}^{H}\mathbf{W}_{AB}^{H}\mathbf{H}\mathbf{F}_{AB}\mathbf{F}_{DB}\mathbf{s} + \mathbf{W}_{DB}^{H}\mathbf{W}_{AB}^{H}\mathbf{n} \tag{2.8}$$

where P is the received power, $\mathbf{s}$ is the data stream vector with the dimension of $n_s \times 1$ such that $\mathbb{E}\{\mathbf{s}\mathbf{s}^{H}\} = \mathbf{I}_{n_s}$ and $\mathbf{n}$ is the additive white Gaussian noise (AWGN) vector whose elements have zero mean and σ^2 variance.

Since there is only one user in the cell, the interference does not occur. Hence, the received signal to noise ratio (SNR) is defined as (El Ayach et al., 2014),

$$\boldsymbol{\gamma} = P\mathbf{R}_{nn}^{-1}\mathbf{W}_{DB}^{H}\mathbf{W}_{AB}^{H}\mathbf{H}\mathbf{F}_{AB}\mathbf{F}_{DB}\mathbf{F}_{DB}^{H}\mathbf{F}_{AB}^{H}\mathbf{H}^{H}\mathbf{W}_{AB}\mathbf{W}_{DB} \tag{2.9}$$

where $\mathbf{R}_{nn} = \sigma^2\mathbf{W}_{DB}^{H}\mathbf{W}_{AB}^{H}\mathbf{W}_{AB}\mathbf{W}_{DB}$ is the noise covariance matrix. Finally, the data rate is calculated as,

$$R = \log_2 |\mathbf{I}_{n_s} + \boldsymbol{\gamma}| \tag{2.10}$$

Analog Beamforming: For the hybrid beamforming scheme, the first consideration is to find the analog precoder ($\mathbf{F}_{AB}$) and the analog combiner ($\mathbf{W}_{AB}$) in such a way that they should maximize the effective channel gain as given by (El Ayach et al., 2014),

$$\mathbf{H}_{eff} = \mathbf{W}_{AB}^H \mathbf{H} \mathbf{F}_{AB} \tag{2.11}$$

where $\mathbf{H}_{eff}$ is called the effective channel matrix with dimension of $M_{RF} \times N_{RF}$ between the transmitter and receiver. In Eq.(2.11), the optimization problem is non-convex since $\mathbf{F}_{AB}$ and $\mathbf{W}_{AB}$ cannot be easily found due to the infinite number of possibilities (Molisch et al., 2017). In order to convert this problem to a convex problem, the codebook based analog beamformer design can be used. From codebook based design, $\mathbf{F}_{AB}$ and $\mathbf{W}_{AB}$ are chosen based on channel array responses which are AoD and AoA, respectively. Furthermore, they can be well constructed by using Orthogonal Matching Pursuit given in Algorithm 1.

Algorithm 1 Analog Beamforming in Algorithm I in (El Ayach et al., 2014)

Require: $\mathbf{F}_{opt}$, $\mathbf{A}$
1: $\mathbf{F}_{AB} = \varnothing$
2: $\mathbf{F}_{res} = \mathbf{F}_{opt}$
3: **for** $i \leq N_{RF}$ **do**
4: $\quad \boldsymbol{\Psi} = \mathbf{A}^H \mathbf{F}_{res}$
5: $\quad k = \arg\max_{s=1,2,\ldots,CS_c} (\boldsymbol{\Psi}\boldsymbol{\Psi}^H)_{s,s}$
6: $\quad \mathbf{F}_{AB} = [\mathbf{F}_{AB} | \mathbf{A}_k]$
7: $\quad \mathbf{F}_{updt} = (\mathbf{F}_{AB}^H \mathbf{F}_{AB})^{-1} \mathbf{F}_{AB}^H \mathbf{F}_{opt}$
8: $\quad \mathbf{F}_{res} = \frac{\mathbf{F}_{opt} - \mathbf{F}_{AB}\mathbf{F}_{updt}}{||\mathbf{F}_{opt} - \mathbf{F}_{AB}\mathbf{F}_{updt}||_F}$
9: **end for**
10: **return** $\mathbf{F}_{AB}$

In Algorithm 1, $\mathbf{F}_{opt}$ is initially obtained from N_{RF} right singular vectors of $\mathbf{H}$. The array response matrix, $\mathbf{A}$ which consists of either AoA or AoD vectors can be obtained from Eq.(2.5) or Eq.(2.6) according to the configuration of antennas. Similarly, the

analog combiner, $\mathbf{W}_{AB}$, can be constructed by using Algorithm 1 by changing N_{RF} to M_{RF}, AoD to AoA and $\mathbf{F}_{opt}$ to $\mathbf{W}_{opt}$ obtaining from M_{RF} left singular vectors of $\mathbf{H}$.

Digital Beamforming: After finding the analog beamformers, the next step is to design the digital beamformers: $\mathbf{F}_{DB}$ and $\mathbf{W}_{DB}$. These beamformers can be chosen for an appropriate scenario such as single user, multiuser, multicell, etc. There are two types of digital beamforming techniques in the literature (Ahmed et al., 2018). One of them is the linear beamforming techniques and the other one is the adaptive beamforming techniques. The linear beamforming techniques have some advantages on the adaptive ones so that they are simpler and widely used in the MIMO systems. They do also not consist of so much complexity and any iteration or update. In fact, adaptive beamforming techniques are more robust and efficient than the linear ones but they are also time consuming and computationally complex techniques. In this thesis, the linear beamforming techniques such as MRT/MRC and singular value decomposition (SVD) are used to provide spectrally efficient systems.

2.3.1. Maximum Ratio Transmission/Combining Beamforming

The first linear precoding technique is the MRT that is one of the most commonly used technique in the literature. It is used for the maximization of the received signal power, however, the MRT is only valid for under $n_s = M_{RF}$ constraint.

For the single user scenario, the MRT precoder can be obtained based on the effective channel matrix given in Eq.(2.11) as,

$$\mathbf{F}_{DB} = \mathbf{H}_{eff}^{H} \tag{2.12}$$

To satisfy the transmit power constraint such that $||\mathbf{F}_{AB}\mathbf{F}_{DB}||_F^2 = 1$, $\mathbf{F}_{DB}$ should be normalized by (El Ayach et al., 2014),

$$\mathbf{F}_{DB} = \frac{\mathbf{F}_{DB}}{||\mathbf{F}_{AB}\mathbf{F}_{DB}||_F} \tag{2.13}$$

At the receiver side, the MRT is called MRC or the matched-filter (MF) combiner that is given as,

$$\mathbf{W}_{DB} = \frac{\mathbf{H}_{eff}\mathbf{F}_{DB}}{||\mathbf{H}_{eff}\mathbf{F}_{DB}||_F} \tag{2.14}$$

2.3.2. SVD Beamforming

In this technique, the most dominant eigenvalues and corresponding eigenvectors are used for the data transmission. Although the singular value decomposition is much computationally complex than MRT, it is valid for all cases $n_s \leq M_{RF}$. Based on Eq.(2.11) for the single user, the SVD of effective channel can be found as,

$$\mathbf{U}\mathbf{\Sigma}\mathbf{V}^H = \mathbf{H}_{eff} \tag{2.15}$$

where $\mathbf{U}$ and $\mathbf{V}$ are unitary matrices which have orthonormal vectors and $\mathbf{\Sigma}$ is the eigenvalue matrix. After that, the SVD (baseline or eigenmode) precoder at the transmitter side, $\mathbf{F}_{DB}$, is calculated as,

$$\mathbf{F}_{DB} = \mathbf{V}_{(1:n_s)} \tag{2.16}$$

where the digital precoder should normalized by Eq. (2.13) to satisfy the transmit power constraint. Similarly, the SVD combiner at the receiver side, $\mathbf{W}_{DB}$, is calculated as,

$$\mathbf{W}_{DB} = \mathbf{U}^H_{(1:n_s)} \tag{2.17}$$

2.4. System Model for Single Cell Multiuser Case

For the multiuser case, we assume that the *K* number of users communicate with a single BS in a single cell. Both the BS and users have multiple antennas. Then, each user

communicates with the BS simultaneously. Since the mmWave MU-MIMO downlink communication is considered, the received signal by the *k*th user is given as (Sun et al., 2018),

$$\begin{aligned}\mathbf{y}_k =& \sqrt{P_k}\mathbf{W}_{DB,k}^H\mathbf{W}_{AB,k}^H\mathbf{H}_k\mathbf{F}_{AB,k}\mathbf{F}_{DB,k}\mathbf{s}_k \\ &+ \sum_{\substack{m=1 \\ (m\neq k)}}^{K} \sqrt{P_k}\mathbf{W}_{DB,k}^H\mathbf{W}_{AB,k}^H\mathbf{H}_k\mathbf{F}_{AB,m}\mathbf{F}_{DB,m}\mathbf{s}_m \\ &+ \mathbf{W}_{DB,k}^H\mathbf{W}_{AB,k}^H\mathbf{n}_k\end{aligned} \tag{2.18}$$

where P_k is the received power by the *k*th user. In Eq.(2.18), the first row is the desired signal whereas the second row is the interference. The last row indicates the noise where $\mathbf{n}_k$ is the AWGN vector for the *k*th user whose elements have zero mean and σ_k^2 variance. The transmit symbol, however, for the *k*th user is denoted as $\mathbf{s}_k$ such that $\mathbb{E}\{\mathbf{s}_k\mathbf{s}_k^H\} = \mathbf{I}_{n_s}$. The effective channel for the *k*th user is defined as,

$$\mathbf{H}_{eff,k} = \mathbf{W}_{AB,k}^H\mathbf{H}_k\mathbf{F}_{AB,k} \tag{2.19}$$

In this case, BS may send multiple data streams to multiple users so that the interference among users and/or data streams can occur. For multiuser case, the signal to interference plus noise ratio (SINR) is calculated as (Sun et al., 2018),

$$\boldsymbol{\gamma}_k = \frac{P_k\mathbf{W}_{DB,k}^H\mathbf{H}_{eff,k}\mathbf{F}_{DB,k}\mathbf{F}_{DB,k}^H\mathbf{H}_{eff,k}^H\mathbf{W}_{DB,k}}{\mathbf{W}_{DB,k}^H\mathbf{W}_{AB,k}^H\left(\sigma_k^2\mathbf{I}_{N_R} + \sum\limits_{\substack{m=1 \\ (m\neq k)}}^{K} P_k\mathbf{H}_k\mathbf{F}_{AB,m}\mathbf{F}_{DB,m}\mathbf{F}_{DB,m}^H\mathbf{F}_{AB,m}^H\mathbf{H}_k^H\right)\mathbf{W}_{AB,k}\mathbf{W}_{DB,k}} \tag{2.20}$$

The data rate of the *k*th user is defined as,

$$R_k = \log_2|\mathbf{I}_{n_s} + \boldsymbol{\gamma}_k| \tag{2.21}$$

For overall system performance, the sum data rate is calculated as,

$$R = \sum_{k=1}^{K} R_k \tag{2.22}$$

Analog Beamforming: For MU-MIMO case, the analog precoders and combiners can be found by using Algorithm 1 for each user in the cell.

Digital Beamforming: The different linear beamforming techniques such as MRT, ZF and MMSE beamformers are used for multiuser case. Especially ZF and MMSE can be used for mitigating the interference among users and/or streams.

2.4.1. Maximum Ratio Transmission/Combining Beamforming

Besides the SU-MIMO case, MRT can also be used for MU-MIMO due to the large number of antenna arrays provide highly directive beams (Swindlehurst et al., 2014).

For the MU-MIMO scenario, the generalized effective channel matrix is obtained by using the effective channel matrix of each user as given in Eq.(2.19) (Sun et al., 2018),

$$\tilde{\mathbf{H}} = [\mathbf{H}_{eff,1}^T \dots \mathbf{H}_{eff,k}^T \dots \mathbf{H}_{eff,K}^T]^T \tag{2.23}$$

where $\tilde{\mathbf{H}}$ is the generalized effective channel matrix with the dimension of $KM_{RF} \times N_{RF}$ that contains all effective channel of users. After that, the generalized MRT precoder $\tilde{\mathbf{F}}_{DB}$ can be determined as,

$$\tilde{\mathbf{F}}_{DB} = \tilde{\mathbf{H}}^H \tag{2.24}$$

where $\tilde{\mathbf{F}}_{DB} = [\mathbf{F}_{DB,1} \dots \mathbf{F}_{DB,k} \dots \mathbf{F}_{DB,K}]$ is the generalized digital precoder matrix which is composed of each user precoder. Equivalently, the *k*th user precoder can also be calculated as,

$$\mathbf{F}_{DB,k} = \mathbf{H}_{eff,k}^H \tag{2.25}$$

To satisfy the transmit power constraint for *k*th user such that $||\mathbf{F}_{AB,k}\mathbf{F}_{DB,k}||_F^2 = 1$, each user precoder should be normalized as (Sun et al., 2018),

$$\mathbf{F}_{DB,k} = \frac{\mathbf{F}_{DB,k}}{||\mathbf{F}_{AB,k}\mathbf{F}_{DB,k}||_F} \tag{2.26}$$

At the receiver side, MRC combiner is given for the *k*th user as,

$$\mathbf{W}_{DB,k} = \frac{\mathbf{H}_{eff,k}\mathbf{F}_{DB,k}}{||\mathbf{H}_{eff,k}\mathbf{F}_{DB,k}||_F} \tag{2.27}$$

2.4.2. Zero Forcing Beamforming

The ZF beamforming is used to mitigate the interference among users as well as data streams. This technique includes matrix inversion in order to mitigate the interference. Thus, it requires much more computation than MRT (Sun et al., 2018).

For the ZF precoder, the generalized effective channel matrix in Eq.(2.23) remains same. Then, the generalized ZF precoder at the transmitter side, $\tilde{\mathbf{F}}_{DB}$ with the dimension of $N_{RF} \times KM_{RF}$, can be calculated as (Sun et al., 2018),

$$\tilde{\mathbf{F}}_{DB} = \tilde{\mathbf{H}}^H(\tilde{\mathbf{H}}\tilde{\mathbf{H}}^H)^{-1} \tag{2.28}$$

where $\tilde{\mathbf{F}}_{DB} = [\mathbf{F}_{DB,1} \dots \mathbf{F}_{DB,k} \dots \mathbf{F}_{DB,K}]$ and each user precoder should be normalized by using Eq. (2.26) for satisfying the transmit power constraint.

2.4.3. Minimum Mean Square Error Beamforming

Since the ZF is mostly affected by the rank deficiency, the minimum mean square error (MMSE) beamforming is alternatively used for preventing the rank deficiencies. The generalized MMSE precoder, $\tilde{\mathbf{F}}_{DB}$ is formulated using Eq.(2.23) given as,

$$\tilde{\mathbf{F}}_{DB} = \tilde{\mathbf{H}}^H(\tilde{\mathbf{H}}\tilde{\mathbf{H}}^H + \beta\mathbf{I}_{N_s})^{-1} \tag{2.29}$$

where β is the regularization factor. It is important to note that the optimal regularization factor is the inverse of received SNR which is P_k/σ_k^2 for the *k*th user.

Similarly in Eq.(2.26), each user precoder shoud be normalized to satisfy the transmit power constraint.

In this thesis, at the user side only MRC combiner is considered instead of the ZF and MMSE combiners because of its simplicity.

2.5. Performance Evaluations

In this section, the simulation results are given to illustrate the effects of different system parameters on the mmWave massive MIMO systems employing hybrid scheme at both end. The important parameters are followings: (1) the number of transmit and receive antennas, (2) the number of users and streams, (3) the selected beamforming method. Also, the detailed mmWave channel parameters for 73GHz frequency are given in Table 2.1 which is obtained from the study of (Samimi and Rappaport, 2016).

Table 2.1. Millimeter-Wave Channel Parameters

Parameter	**Description**	**LoS**	**nLoS**	**Distributions**
C	Number of Cluster	1	1-6	Discrete Uniform
S_c	Number of Subpaths for each cluster	1	1-30	Discrete Uniform
$\mu_{AoD}[^\circ]$	Mean AoD angles	-12.6	-4.9	Uniform (0,360), Gaussian
$\sigma_{AoD}[^\circ]$	Standard deviation AoD angles	5.9	4.5	Uniform (0,360), Gaussian
$\mu_{AoA}[^\circ]$	Mean AoA angles	10.8	3.6	Uniform (0,360), Gaussian
$\sigma_{AoA}[^\circ]$	Standard deviation AoA angles	5.3	4.8	Uniform (0,360), Gaussian
$\sigma_{\phi,AoD}[^\circ]$	Standard deviation AoD for azimuth angles	2.5	3.5	Gaussian, Laplacian
$\sigma_{\theta,AoD}[^\circ]$	Standard deviation AoD for elevation angles	8.5	7.0	Gaussian, Laplacian
$\sigma_{\phi,AoA}[^\circ]$	Standard deviation AoA for azimuth angles	11.5	3.5	Gaussian, Laplacian
$\sigma_{\theta,AoA}[^\circ]$	Standard deviation AoA for elevation angles	10.5	6.0	Gaussian, Laplacian

While performing the simulations, a small cell (pico or femto) having one BS that serves to single or multiple users is considered. For the small cell assumption, we assume that the LoS link occur in every time slots (trial) for each user. Hence, this is a proper

scenario for the mmWave communication. Furthermore, the simulation parameters for detailed information are given in Table 2.2 and the SNR in the plots is defined as either SNR = P/σ^2 for SU-MIMO case or SNR$_k$ $= P_k/\sigma_k^2$ assuming each user have the same SNR value for MU-MIMO case.

Figure (2.2) shows that the effects of multiple streams on the data rate for the single user. When the number of streams increases, the data rate increases as well. In this case, we increase the number of RF chains at the BS to transmit more streams.

In the Figure (2.3), it is observed that increasing the number of antennas at both transmitter and receiver enhance the data rate. The data rate can be further improved by increasing the receive antennas.

Table 2.2. Simulation Parameters for Single Cell mmWave MIMO Systems

Parameter	**Description**	**Value**
P_{LoS}	Probability of LoS	1
K	Number of users	[1,2,10,20,40]
N_R	Number of antennas at users	8
N_T	Number of antennas at BS	128
M_{RF}	Number of RF chains at users	[1,2,3,4]
N_{RF}	Number of RF chains at BS	[1,2,3,4,10,20,40]
n_s	Number of stream for each user	[1,2,3,4]
N_s	Number of stream at BS	Kn_s

In the Figure (2.4), the data rate enhances when both the transmit and receive antennas increase.

After showing the SU-MIMO mmWave communications, we focus on the MU-MIMO mmWave communications. The sum data rate is provided for MRT precoder with different number of users and streams in the Figure (2.5). As the number of streams increases, the sum data rate increases as well. Besides that, if the number of users increases the sum data rate also increases.

The sum data rate is drawn for MMSE precoder in Figure (2.6) with the same parameters as in Figure (2.5). While the differences on the sum data rate between MRT precoder and MMSE precoder are indistinguishable when the $n_s = 1$, MMSE precoder shows its superiority against MRT on the sum data rate when the multiple streams, $n_s = 2$, are employed.

The data rate per user can be examined to observe how the average data rate for

each user is affected by the different precoders. Hence, the data rate per user is provided for MRT and ZF precoders with different number of users and $n_s = 2$ in the Figure (2.7). When $K = 2$, MRT outperforms ZF in the low SNR regime (<15dB), while MRT and ZF precoders provide the same performance in the high SNR region. As the number of users increases, the ZF outperforms MRT precoding since it mitigates the interference among users or streams.

As a summary, the ZF and MMSE precoders should be taken into consideration for the systems in which a large number of users exists. It is also worth noting that, the performance of MRT precoder can be improved by increasing the number of antennas at the BS. As the large antenna arrays provide higher directivity so the occurrence of any interference among users is reduced. For the ultra large antenna systems, MRT can also be a good alternative in mmWave MIMO systems.

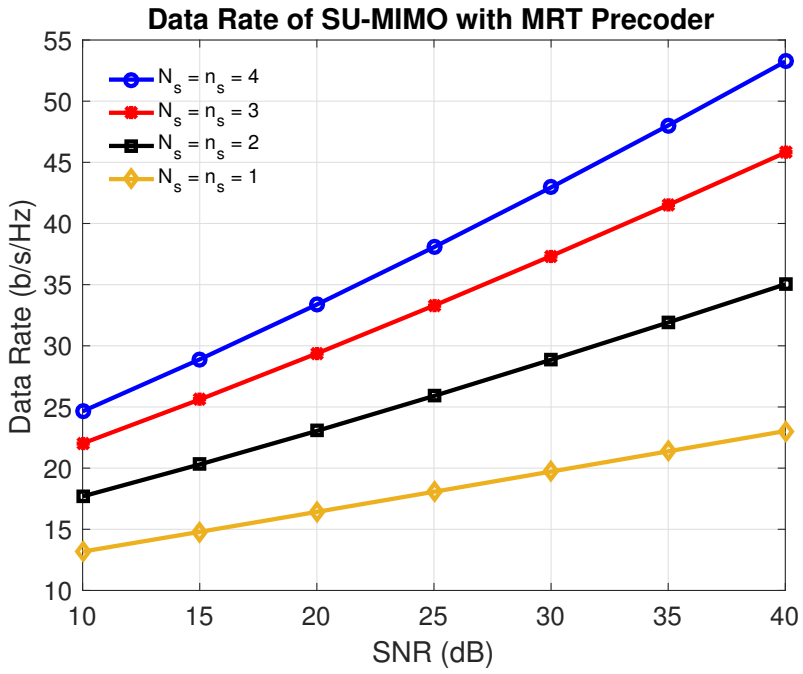

Figure 2.2. Effects of the number of streams for SU-MIMO via MRT precoder.

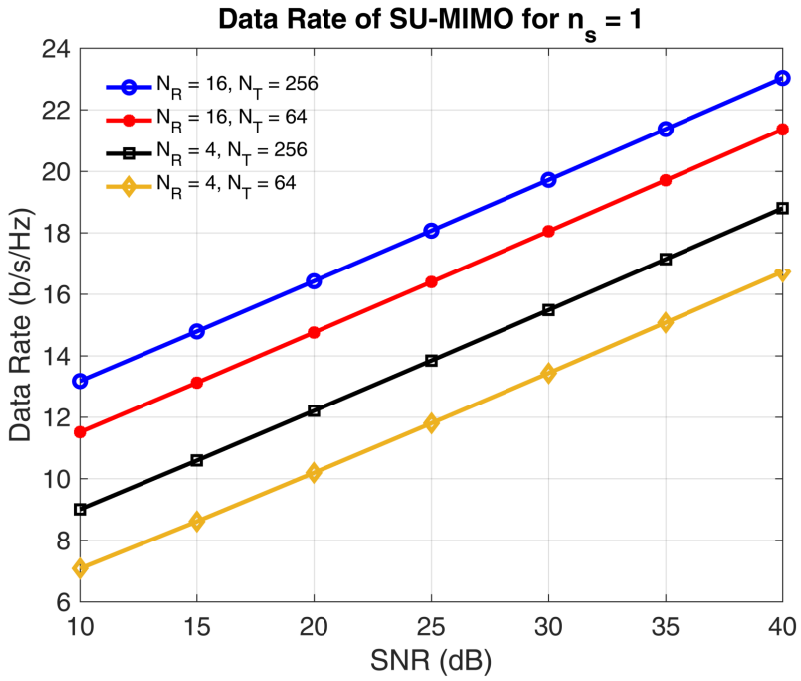

Figure 2.3. Effects of N_T and N_R for SU-MIMO via MRT precoder and $n_s = 1$.

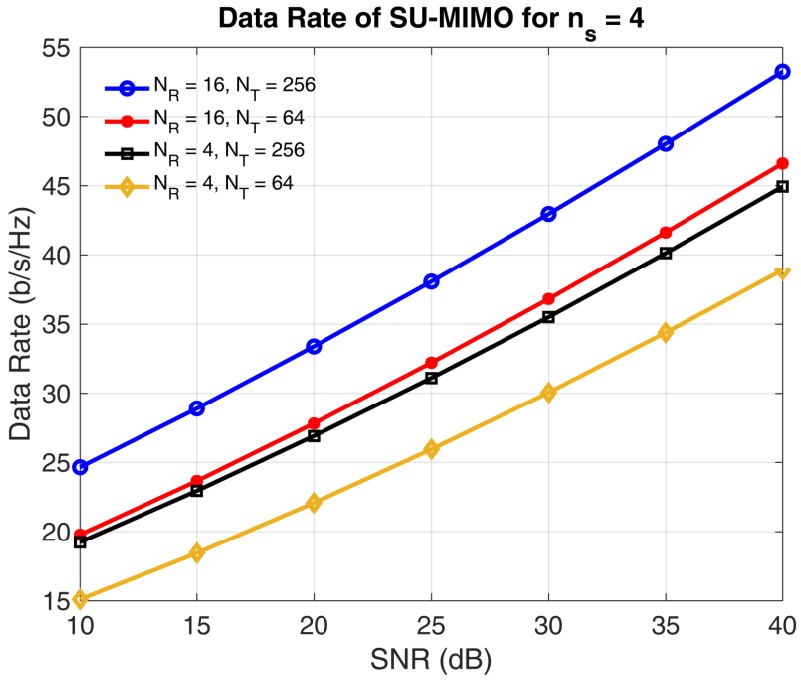

Figure 2.4. Effects of N_T and N_R for SU-MIMO via MRT precoder and $n_s = 4$.

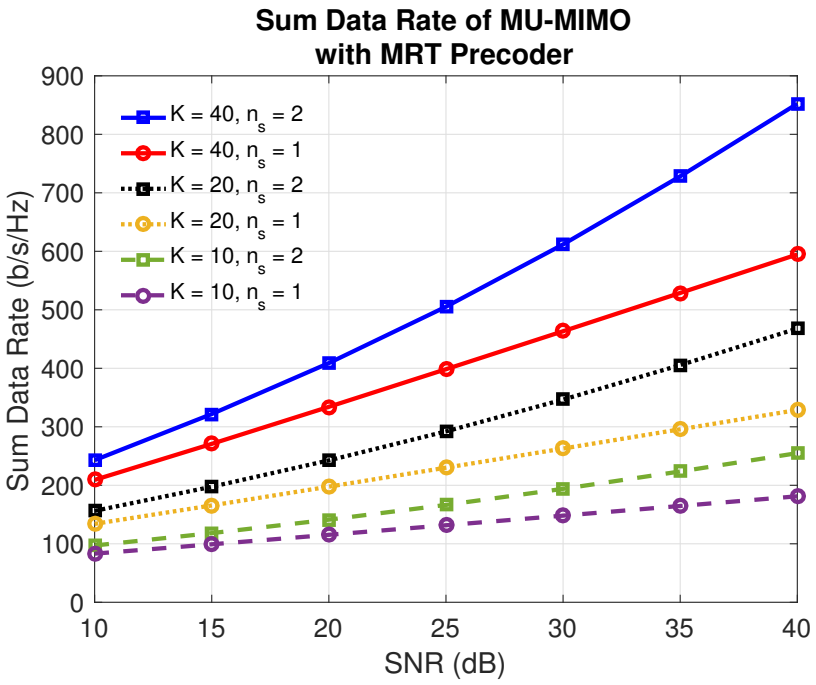

Figure 2.5. Sum data rate of MU-MIMO system vs K and n_s with MRT precoder.

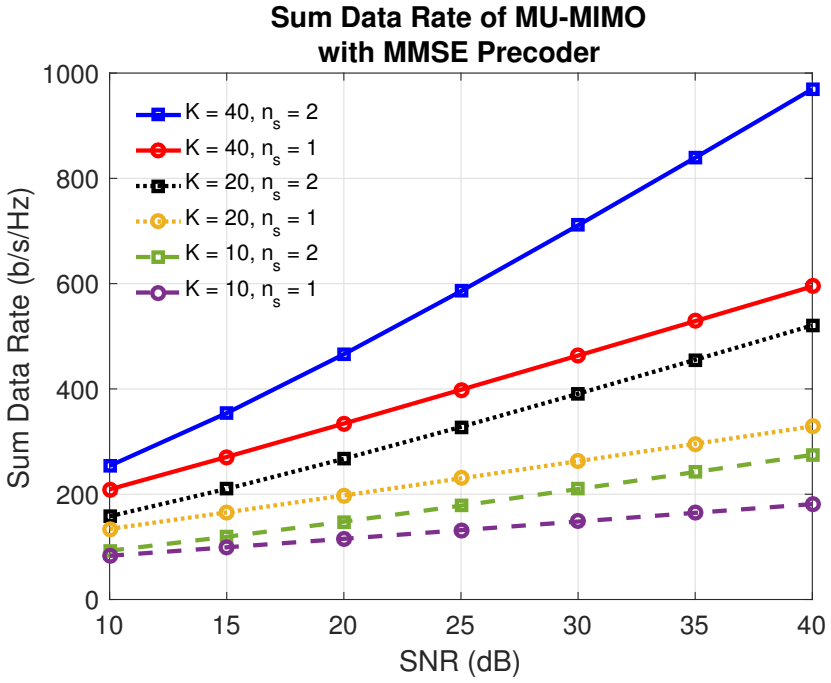

Figure 2.6. Sum data rate of MU-MIMO system vs K and n_s with MMSE precoder.

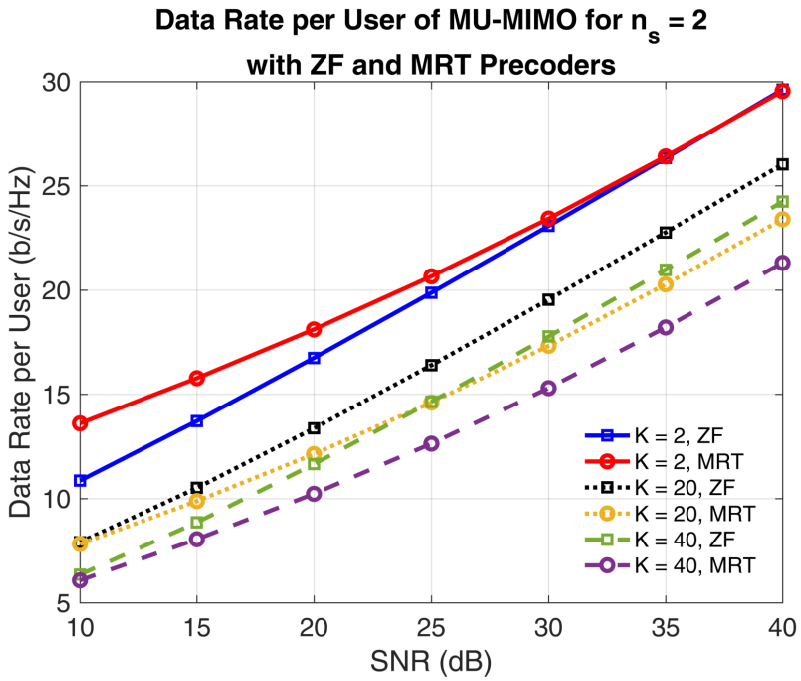

Figure 2.7. Data rate per user of MU-MIMO system vs K with ZF and MRT precoders.

CHAPTER 3

SECURE SINGLE CELL MULTIUSER MIMO SYSTEMS

Over the last decade, wireless data traffic has dramatically increased with the increasing number of smart devices such as IoT, unmanned vehicles, and drones. On one hand, these smart devices have supported diverse applications from medical to commercial or military industries. On the other hand, they have caused security concerns as well. Since the cryptographic techniques applied in the upper layers, the PLS has been examined in the literature as a complementary solution at the physical layer. In this chapter, we propose a PLS concept for mmWave MU-MIMO systems in a single cell via the hybrid beamforming techniques (Erdoğan et al., 2020).

The organization of this chapter is as follows: we first give a brief information about beackground of PLS in Section 3.1. Then, we introduce the system model and propose a secure scheme for single cell mmWave MU-MIMO communication in Section 3.2 and Section 3.3, respectively. Finally, we give the simulation results in Section 3.4.

3.1. Background

The first information-theoretic security consideration was proposed by Shannon in his pioneering work (Shannon, 1949). In Shannon's study, three-node network topology including transmitter, legitimate receiver and eavesdropper that are often referred to as 'Alice', 'Bob' and 'Eve' was introduced. Shannon presented a secure system where a single private key was generated and it was used at both 'Alice' and 'Bob' for encryption and decryption process. This study has provided a significant improvement in the communication systems. Moreover, cryptography has emerged as a new research field.

After Shannon's work, Wyner studied to secure communication over random noise channels and examined the *wiretap* channel in (Wyner, 1975). According to Wyner, the messages could be encoded into codewords that consist of a sufficiently large number of symbols and sent them to the legitimate receiver. While the legitimate receiver could get a degraded version of the original message, the eavesdropper could obtain the more

degraded version of the original message via the wiretap channel. The codewords could provide secure communication on the noisy channels if the codewords were sufficiently large.

Csiszár and Körner further improved this idea and applied it to the broadcast channel with two receivers that were 'Bob' and 'Eve' instead of wiretap channel (Csiszár and Korner, 1978). From their points of view, they mathematically expressed the secrecy capacity as a difference of the legitimate receiver capacity and the eavesdropper capacity. This showed us a significant impact on the channel state information (CSI) of the eavesdropper. In this case, if the CSI of eavesdropper is known by the transmitter (CSIT), the perfect secrecy can be provided.

PHY security has been extensively studied in the literature for both the information-theoretic perspective and the signal processing perspective. We follow these signal processing approaches throughout this thesis. The signal processing approaches for the security systems are mainly considered as beamforming techniques via the multiple antennas either used at only the transmitter side (MISO) or both sides (MIMO).

From the study of (Ng et al., 2014), the passive eavesdropper without its CSI has been considered with AN beamformer for the systems that is wireless information and power transmission. The precoders of legitimate users have been obtained by solving a convex optimization problem. However, the system does not include the mmWave channel and hybrid architecture. In (Ju et al., 2017), the authors have studied three-node network topology in mmWave communication system in which the passive eavesdropper has been considered. Although MRT precoder combining with AN has employed to degrade the channel of the eavesdropper, the hybrid scheme has not used at both ends. For the MISO-OFDM system, the authors in (Ramadan et al., 2017) have examined two different methods for constructing appropriate digital precoders namely secrecy outage minimization MRT precoder and secrecy throughput maximization MRT precoder. In this system, the hybrid scheme has employed at only the transmitter side and the system secrecy has carried out without using AN. Another study for the PLS has been given in (Xu et al., 2019). In this study, three-node network topology has been considered for the mmWave system and each of nodes has employed the hybrid architecture. The AN beamformer has been used for the passive eavesdropper. The antenna selection technique has considered for both AN and the legitimate user precoder. In (Tian et al., 2017), the mmWave sys-

tem employed hybrid schemes at each node has been considered as a downlink MIMO communication scenario. The system has had three-nodes for a single user case. Both full-CSIT and no-CSIT of eavesdropper has been examined. For no-CSIT case, the AN beamformer has been employed. The SVD beamforming has also been applied both for precoder and combiner of the legitimate user. Finally, the secure mmWave multiuser MIMO system have been analyzed in (Wang et al., 2019). Although the hybrid architecture has employed at both transmitter and relay only, the analog architecture has used for each user. Besides the AN used to jam the channel of eavesdroppers, the precoders for the multiuser have been chosen as ZF to mitigate the interference.

In the literature, both the single user MIMO systems with AN and multiuser MISO systems with AN have examined for secure mmWave communications. However, multiuser MIMO systems through hybrid beamforming are not studied well according to the best of our knowledge. Hence, we proposed a secure mmWave multiuser MIMO communication by employing the hybrid beamforming architecture in this chapter. We present how AN beamformer can be obtained in such a way that it is chosen from the null-space of the combination of analog and digital precoders. Thus, we provide a degradation of the channel of eavesdropper using AN beamformer. The precoder is selected as MMSE to mitigate interference and avoid the rank deficiency. At the receiver side, the postcoders are selected as MRC since it is simple to use and requires no more complexity.

3.2. System Model

We consider a small cell (pico, femto, etc.) downlink secure MU-MIMO mmWave communication scenario shown in Figure (3.1). Each legitimate user communicates with the BS over both LoS and NLoS links and this system is a highly proper scenario for small cell networks. There is one passive eavesdropper that tries to obtain message signals from channels of each legitimate user. Assume that each legitimate user and the eavesdropper can share some specific AoDs. To provide this, we randomly select some AoDs among AoDs of legitimate users for the eavesdropper.

In this mmWave communication system, there is K number of legitimate users each of them is equipped with N_R antennas in the single cell which has only one BS is equipped with N_T antennas. On the other hand, only one eavesdropper is considered since

we assume that multiple antenna eavesdropper can gain information from the channel of each legitimate user.

Under considered scenario, each node in the cell (BS, legitimate users and eavesdropper) employs the hybrid beamforming architecture shown in Figure (3.2).

Since hybrid beamforming is employed at both the transmitter and receiver sides, the digital precoder is given as $\mathbf{F}_{DB} \in \mathbb{C}^{N_{RF} \times N_s}$ and the analog precoder is given as $\mathbf{F}_{AB} \in \mathbb{C}^{N_T \times N_{RF}}$ where N_T, N_{RF} and N_s are the number of transmit antennas, the number of RF chains and the number of data streams at the transmitter, respectively.

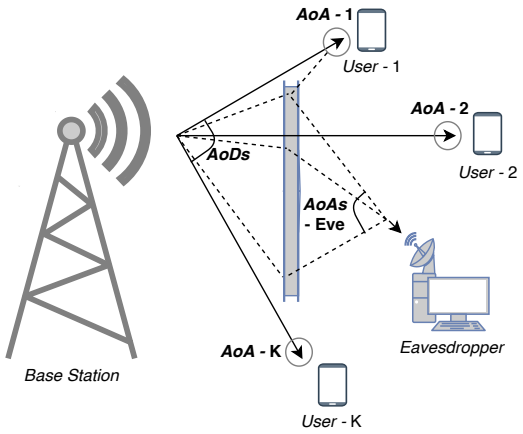

Figure 3.1. Secure mmWave single cell MU-MIMO downlink communications.

Following transmit hybrid scheme, we consider receive hybrid scheme in Figure (3.2) such that the analog combiner is $\mathbf{W}_{AB} \in \mathbb{C}^{N_R \times M_{RF}}$ and the digital combiner is $\mathbf{W}_{DB} \in \mathbb{C}^{M_{RF} \times n_s}$ where N_R, M_{RF} and n_s are the number of receive antennas, the number of RF chains and the number of data streams at the receiver, respectively.

After we introduce the hybrid arhitecture, we have assumed that the CSI of eavesdropper are not known at the BS since the eavesdropper is a passive node that wants to hide its presence from the BS. In this case, we utilize the AN beamforming to jam the channel of eavesdropper.

3.3. The Proposed Scheme

We propose a novel secure scheme which builds properly up the AN beamforming considering hybrid architecture in Figure (3.2) (Erdoğan et al., 2020).

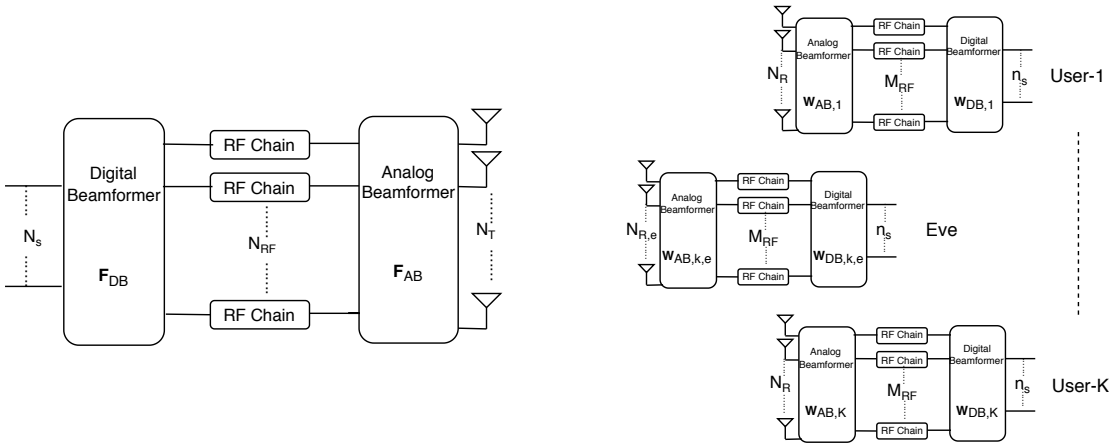

Figure 3.2. Hybrid beamforming for secure mmWave MU-MIMO communications.

The most commonly used method for finding AN precoder in the literature is to select it from the null-space of digital precoder consisting of each user precoder (Wang et al., 2018). Since we consider the hybrid scheme, we first have to find the additional analog precoders to transmit AN signal. In fact, the analog precoder for AN can be constructed randomly with selecting random angles of AoDs (Wang et al., 2019). However, the computational complexity required for analog and digital parts of AN can increase if the number of users increases in the cell. The sake of simplicity, we propose the new method with following equations. At this point of view, the transmit signal with AN precoder is given by,

$$\overline{\mathbf{x}} = \sqrt{\phi}\mathbf{F}_{AB}\mathbf{F}_{DB}\mathbf{s} + \sqrt{1-\phi}\mathbf{F}_{AN}\mathbf{z} \tag{3.1}$$

where $\mathbf{F}_{AN} \in \mathbb{C}^{N_T \times N_{RF} - KM_{RF}}$ is the AN precoder matrix, $\mathbf{s} \in \mathbb{C}^{N_s \times 1}$ is the transmit symbol such that $\mathbb{E}\{\mathbf{s}\mathbf{s}^H\} = \mathbf{I}_{N_s}$, $\mathbf{z}$ is the artificial gaussian noise stream $\mathcal{CN}(0,1)$ and ϕ is the power allocation factor between $\mathbf{s}$ and $\mathbf{z}$. The received signal for the *k*th legitimate user can be given by, (Sun et al., 2018)

$$\begin{aligned}\mathbf{y}_k =& \sqrt{\phi P_k}\mathbf{W}_{DB,k}^H\mathbf{W}_{AB,k}^H\mathbf{H}_k\mathbf{F}_{AB,k}\mathbf{F}_{DB,k}\mathbf{s}_k \\ &+ \sum_{\substack{j=1 \\ (j\neq k)}}^{K} \sqrt{\phi P_k}\mathbf{W}_{DB,k}^H\mathbf{W}_{AB,k}^H\mathbf{H}_k\mathbf{F}_{AB,j}\mathbf{F}_{DB,j}\mathbf{s}_j \\ &+ \sqrt{(1-\phi)P_k}\mathbf{W}_{DB,k}^H\mathbf{W}_{AB,k}^H\mathbf{H}_k\mathbf{F}_{AN}\mathbf{z} \\ &+ \mathbf{W}_{DB,k}^H\mathbf{W}_{AB,k}^H\mathbf{n}_k\end{aligned} \tag{3.2}$$

where P_k is the received power for the *k*th legitimate user, $\mathbf{H}_k \in \mathbb{C}^{N_R \times N_T}$ is the channel matrix between BS and *k*th legitimate user and $\mathbf{n}_k$ is the complex AWGN with zero mean and σ_k^2 variance, $\mathcal{CN}(0, \sigma_k^2)$. The $\mathbf{W}_{DB,k}$ and $\mathbf{W}_{AB,k}$ are the $M_{RF} \times n_s$ digital combiner and $N_R \times M_{RF}$ analog combiner for the *k*th legitimate user, respectively. Since we consider the MMSE precoder that mitigates the interference among users and streams, the generalized $N_T \times N_{RF}$ analog and $N_{RF} \times N_s$ digital precoders are $\mathbf{F}_{AB}$ and $\mathbf{F}_{DB}$ while $\mathbf{F}_{AB,k}$ and $\mathbf{F}_{DB,k}$ are the $N_T \times M_{RF}$ analog precoder and $M_{RF} \times n_s$ digital precoder for the *k*th legitimate user where M_{RF} and n_s are selected from N_{RF} and N_s for the corresponding *k*th legitimate user, respectively. We note that, a reliable communication is provided under $KM_{RF} \leq N_{RF}$ constraint.

On the other side, the received signal by the eavesdropper from the *k*th legitimate user is also given as,

$$\begin{aligned}\mathbf{y}_{e,k} = &\sqrt{\phi P_k}\mathbf{W}_{DB,e,k}^H\mathbf{W}_{AB,e,k}^H\mathbf{H}_{e,k}\mathbf{F}_{AB,k}\mathbf{F}_{DB,k}\mathbf{s}_k \\ &+ \sum_{\substack{j=1 \\ (j\neq k)}}^{K} \sqrt{\phi P_k}\mathbf{W}_{DB,e,k}^H\mathbf{W}_{AB,e,k}^H\mathbf{H}_{e,k}\mathbf{F}_{AB,j}\mathbf{F}_{DB,j}\mathbf{s}_j \\ &+ \sqrt{(1-\phi)P_k}\mathbf{W}_{DB,e,k}^H\mathbf{W}_{AB,e,k}^H\mathbf{H}_{e,k}\mathbf{F}_{AN}\mathbf{z} \\ &+ \mathbf{W}_{DB,e,k}^H\mathbf{W}_{AB,e,k}^H\mathbf{n}_{e,k}\end{aligned} \tag{3.3}$$

For the hybrid beamforming scheme, the analog precoder $\mathbf{F}_{AB,k}$ and combiner $\mathbf{W}_{AB,k}$ for the *k*th legitimate user and the analog combiner $\mathbf{W}_{AB,e,k}$ for the eavesdropper are determined by using Eq.(2.11) in Section 2, respectively. After finding the analog beamformers, the digital precoder $\mathbf{F}_{DB,k}$ for the *k*th legitimate user can be provided by using Eq.(2.29) since the MMSE precoder is chosen for mitigating the interference.

Considering the proposed hybrid scheme for the AN precoder, the AN precoder is jointly chosen from the null-space of analog and digital precoders by taking the singular value decomposition such that

$$\bar{\mathbf{U}}\bar{\mathbf{\Sigma}}\bar{\mathbf{V}}^H = \overline{\mathbf{F}} \tag{3.4}$$

where $\overline{\mathbf{F}} = [(\mathbf{F}_{AB,1}\mathbf{F}_{DB,1}) \dots (\mathbf{F}_{AB,K}\mathbf{F}_{DB,K})]$.Then, the proposed AN precoder can be

obtained as,

$$\mathbf{F}_{AN} = \bar{\mathbf{U}}_{(:,KM_{RF}+1:N_{RF})} \tag{3.5}$$

It is important to note that we set $M_{RF} = n_s$ to reduce the required computation time. After finding the digital precoders and AN precoder, the digital combiner $\mathbf{W}_{DB,k}$ for the *k*th legitimate user can be given by Eq.(2.27) and the corresponding eavesdroppers' digital combiner $\mathbf{W}_{DB,e,k}$ can be obtained as,

$$\mathbf{W}_{DB,e,k} = \frac{\mathbf{W}_{AB,e,k}^H \mathbf{H}_{e,k} \mathbf{F}_{AB,k} \mathbf{F}_{DB,k}}{||\mathbf{W}_{AB,e,k}^H \mathbf{H}_{e,k} \mathbf{F}_{AB,k} \mathbf{F}_{DB,k}||_F} \tag{3.6}$$

It should be noted that the Eq.(3.6) is the worst case for the *k*th legitimate user since the eavesdropper utilizes precoding matrices of each legitimate user.

Following all matrices, the SINR is evaluated for the *k*th legitimate user given as,

$$\boldsymbol{\gamma}_k = \frac{\phi P_k \mathbf{W}_{DB,k}^H \mathbf{W}_{AB,k}^H \mathbf{H}_k \mathbf{F}_{AB,k} \mathbf{F}_{DB,k} \mathbf{F}_{DB,k}^H \mathbf{F}_{AB,k}^H \mathbf{H}_k^H \mathbf{W}_{AB,k} \mathbf{W}_{DB,k}}{\mathbf{W}_{DB,k}^H \mathbf{W}_{AB,k}^H \left(P_k \mathbf{H}_k \left(\phi \mathbf{D}_k + (1-\phi) \mathbf{F}_{AN} \mathbf{F}_{AN}^H\right) \mathbf{H}_k^H + \sigma_k^2 \mathbf{I}_{N_R}\right) \mathbf{W}_{AB,k} \mathbf{W}_{DB,k}} \tag{3.7}$$

where $\mathbf{D}_k$ is the effective interference matrix with the dimension of $N_T \times N_T$ for the *k*th legitimate user and it is calculated as,

$$\mathbf{D}_k = \sum_{\substack{j=1 \\ (j \neq k)}}^{K} \mathbf{F}_{AB,j} \mathbf{F}_{DB,j} \mathbf{F}_{DB,j}^H \mathbf{F}_{AB,j}^H \tag{3.8}$$

We further assume that the eavesdropper can cancel out the inter-user interference given Eq. (3.3). Thus, the SINR of corresponding eavesdropper is calculated as,

$$\boldsymbol{\gamma}_{e,k} = \frac{\phi P_k \mathbf{W}_{DB,e,k}^H \mathbf{W}_{AB,e,k}^H \mathbf{H}_{e,k} \mathbf{F}_{AB,k} \mathbf{F}_{DB,k} \mathbf{F}_{DB,k}^H \mathbf{F}_{AB,k}^H \mathbf{H}_{e,k}^H \mathbf{W}_{AB,e,k} \mathbf{W}_{DB,e,k}}{\mathbf{W}_{DB,e,k}^H \mathbf{W}_{AB,e,k}^H \left((1-\phi) P_k \mathbf{H}_{e,k} \mathbf{F}_{AN} \mathbf{F}_{AN}^H \mathbf{H}_{e,k}^H + \sigma_{e,k}^2 \mathbf{I}_{N_R}\right) \mathbf{W}_{AB,e,k} \mathbf{W}_{DB,e,k}} \tag{3.9}$$

The data rate of the *k*th legitimate user can be calculated as,

$$R_k = \log_2 |\mathbf{I}_{n_s} + \boldsymbol{\gamma}_k| \tag{3.10}$$

The corresponding eavesdropper's data rate can be given as,

$$R_{e,k} = \log_2 \left|\mathbf{I}_{n_s} + \boldsymbol{\gamma}_{e,k}\right| \tag{3.11}$$

Finally, the average secrecy rate of the *k*th legitimate user is defined by (Wang et al., 2018),

$$R_k^s = \mathbb{E}\{[R_k - R_{e,k}]^+\}, \quad k = 1, \ldots, K \tag{3.12}$$

where $[x]^+ \triangleq \max\{0, x\}$. Then, the average secrecy sum rate is given as,

$$R_s = \sum_{k=1}^{K} R_k^s \tag{3.13}$$

Another metric for measuring to system security is the secrecy outage probability. An outage probability for the *k*th legitimate user given with threshold secrecy rate (R_{th}) is calculated as,

$$\mathrm{P}(R_k^s < R_{th}) \tag{3.14}$$

3.4. Performance Evaluations

The simulation results are provided to illustrate the system performance in terms of average secrecy sum rate and secrecy outage probability. The average SNR in the

plots is defined as $\text{SNR}_k = P_k/\sigma_k^2$ assumed that SNR_k is the same for all users. The key simulation parameters are given in Table 3.1 and mmWave channel parameters are given in Table 2.1. All simulation results are obtained by using Monte Carlo Simulations.

Table 3.1. Simulation Parameters for Secure Single Cell mmWave MU-MIMO Systems

Parameter	**Description**	**Value**
K	Legitimate users	[5,10,15,20,30]
N_T	BS antennas	128
N_R	User antennas	8
$N_{R,e}$	Eavesdropper antennas	256
N_{RF}	BS RF chains	32
M_{RF}	User RF chains	[1,2] $= n_s$ with $(KM_{RF} \leq N_{RF})$
n_s	Data stream for each user	[1,2]
N_s	Data stream for BS	Kn_s

In Figure (3.3), a single stream ($n_s = 1$) and multi stream ($n_s = 2$) are assigned to each legitimate user. The optimum power factor (ϕ) is determined for different n_s and SNR values for $K = 5$. In the low SNR regime, the average secrecy rate per user decreases due to the usage of AN beamformer. Contrarily, using AN beamformer can improve the average secrecy rate per user in the high SNR regime. In both low and high SNR regime, single stream provides more security than multi streams because the eavesdropper can obtain the information from only on the AoDs of nLoS but not the LoS. Since we assume that the channel of each legitimate user has both LoS and nLoS components, we can send the multiple streams via nLoS components together with LoS component. Thus, the eavesdropper can gain more information from the nLoS links.

For Figures (3.4) and (3.5), the average secrecy rate per user is observed for the $n_s = 1, 2$ with $K = 10$ and $K = 15$ users, respectively. Similar to Figure (3.3), sending the single stream from the LoS connection is more wisely in the low SNR regime while the multiple streams can enhance the system secrecy in the high SNR regime.

In Figure (3.6), the average secrecy rate per user is shown for two different number of users, $K = 20, 30$, with $n_s = 1$ stream and three different SNR values. The performance results show that the average secrecy rate per user decreases as the number of users increases. Because the total transmit power in the BS is allocated to higher number of users. In the high SNR regime, the more power allocated to AN provides secrecy enhancement on the system.

For Figures (3.7) and (3.8), the average secrecy sum rate are drawn on the different number of users, $K = 5, 10, 15$, with their optimum power factors which are determined before for $n_s = 1$ and $n_s = 2$ case, respectively. In both figures, the average secrecy sum rate increases as the number of legitimate users increases as well. The average secrecy sum rate is enhanced by increasing SNR when $n_s = 2$ while the average secrecy sum rate is slightly increased for $n_s = 1$ when the average SNR is getting high.

In Figure (3.9), the average secrecy sum rate is shown for higher number of legitimate users, $K = 10, 20, 30$, with their optimum power factors and $n_s = 1$ stream. When the number of legitimate users increases, the average secrecy sum rate increases as well.

The secrecy outage probability is a powerful tool on the system security. We select the optimal power allocation values determined in Figures (3.3)-(3.5) at 25dB SNR for the sake of simplicity while obtaining the outage probability results.

Figure (3.10) draws the secrecy outage probability with respect to SNR for the two different threshold rates and three different number of users. When $n_s = 1$ and $R_{th} = 5$ b/s/Hz, the secrecy outage probability is improved and gives almost the same performance for three different number of users in high SNR region. While the outage definitely occurs in the low SNR region when $R_{th} = 15$ b/s/Hz, the secrecy can still be provided at the lower threshold rate, $R_{th} = 5$ b/s/Hz, at the same SNR region. In Figure (3.11), the secrecy outage probability is getting poor when the number of streams increases for $n_s = 2$ compared to the single stream case.

In Figure (3.12), the effects of higher number of users with their optimal power allocation values and two different threshold rates are examined. The secrecy outage probability is getting poor even for $R_{th} = 5$ b/s/Hz, as the number of users increases.

For Figure (3.13), the secrecy outage probability is directly proportional to the number of users while it is also inversely proportional to the number of antennas as given in Figure (3.14). The secrecy outage probability is improved as the number of antennas increases. Otherwise, the eavesdroppers at which have more antennas make the secrecy outage probability worse as illustrated in Figure (3.15).

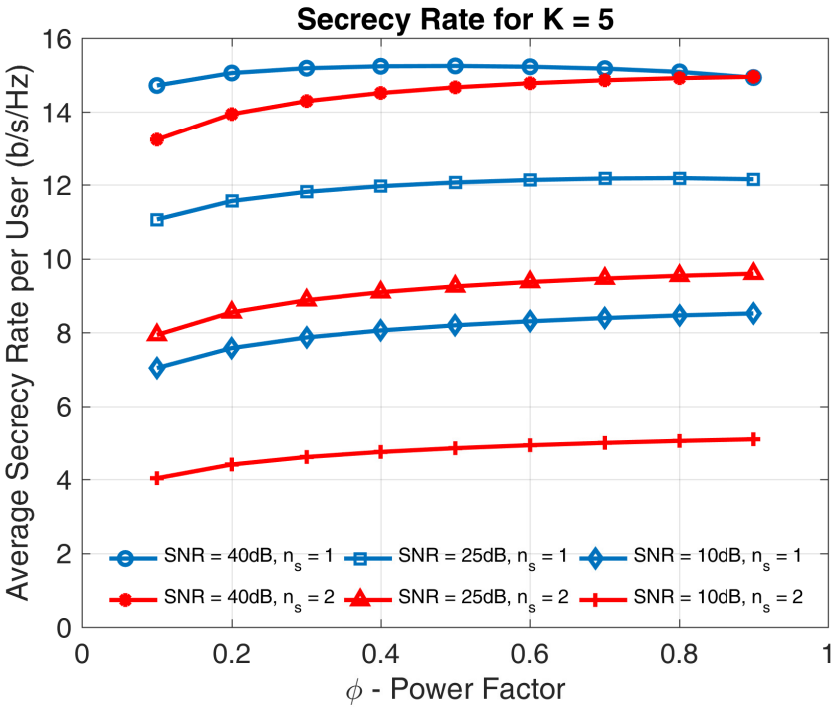

Figure 3.3. Average secrecy rate per user vs ϕ for K = 5.

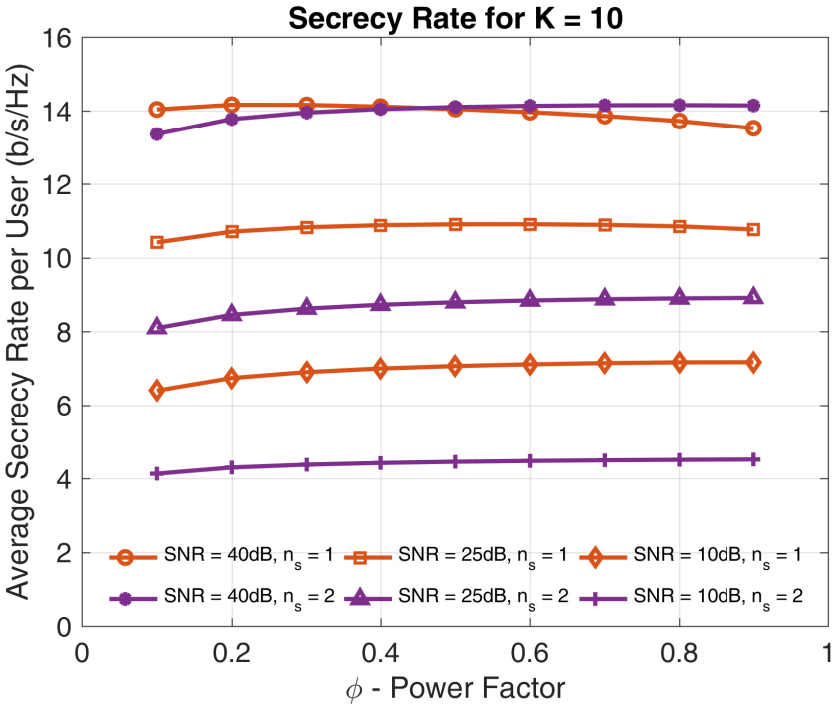

Figure 3.4. Average secrecy rate per user vs ϕ for K = 10.

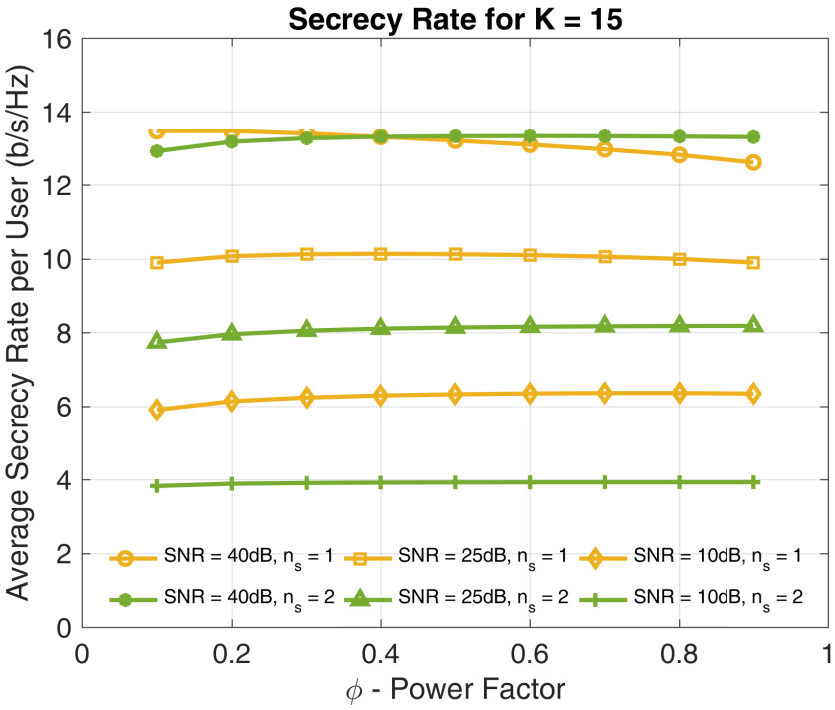

Figure 3.5. Average secrecy rate per user vs ϕ for K = 15.

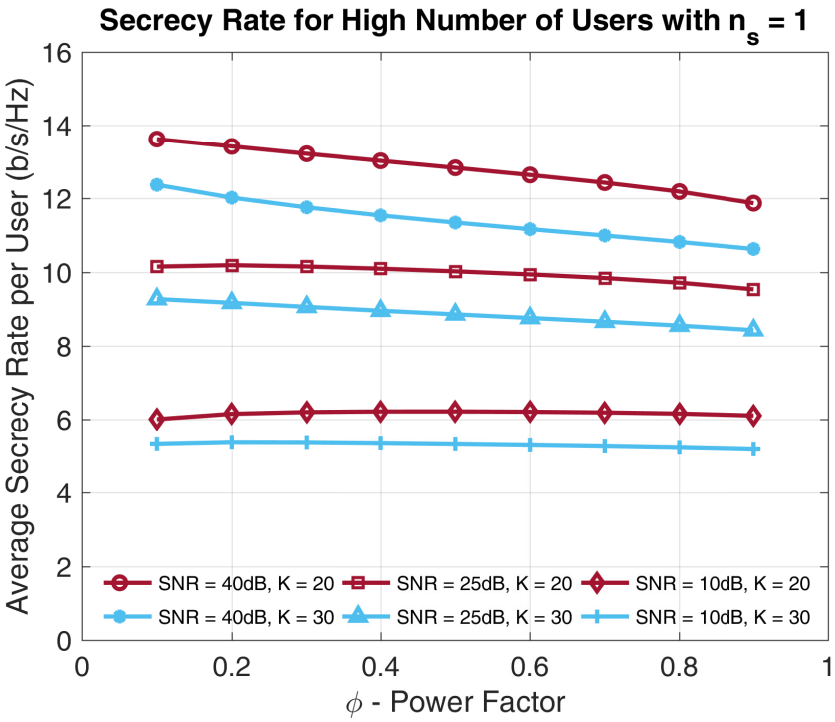

Figure 3.6. Average secrecy rate per user vs ϕ and K for $n_s = 1$.

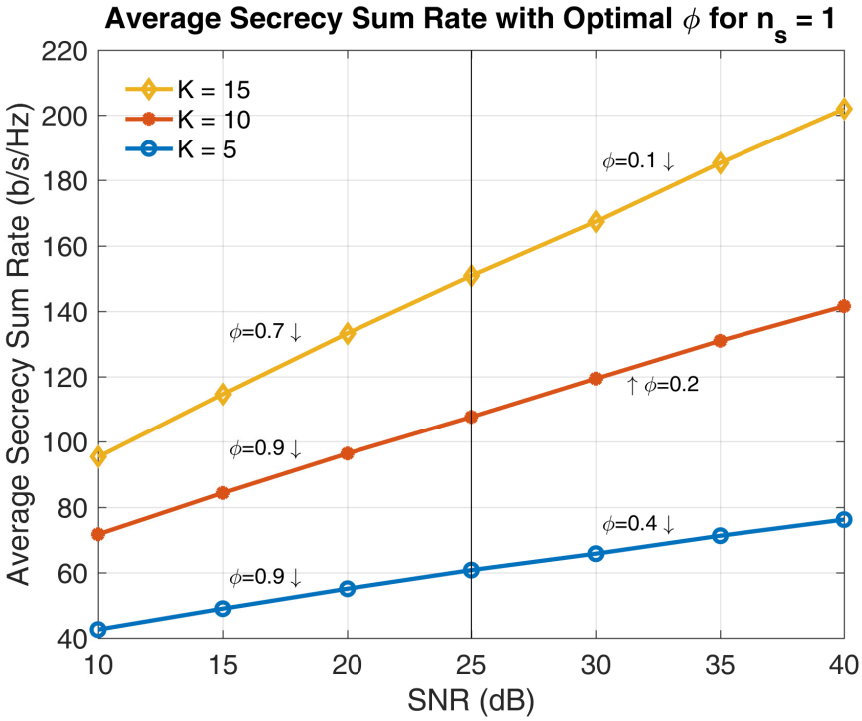

Figure 3.7. Average secrecy sum rate vs SNR and K for $n_s = 1$.

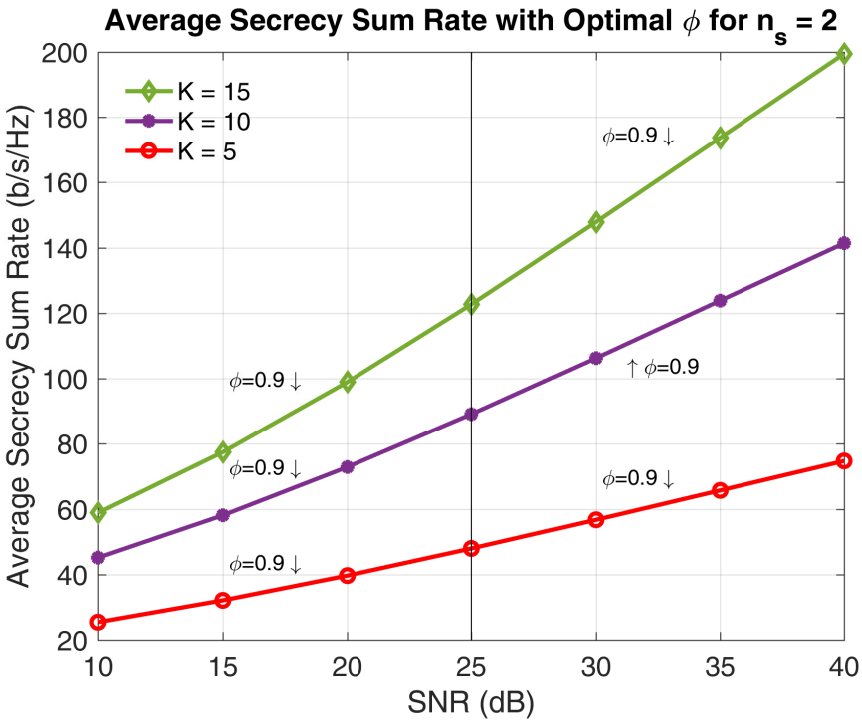

Figure 3.8. Average secrecy sum rate vs SNR and K for $n_s = 2$.

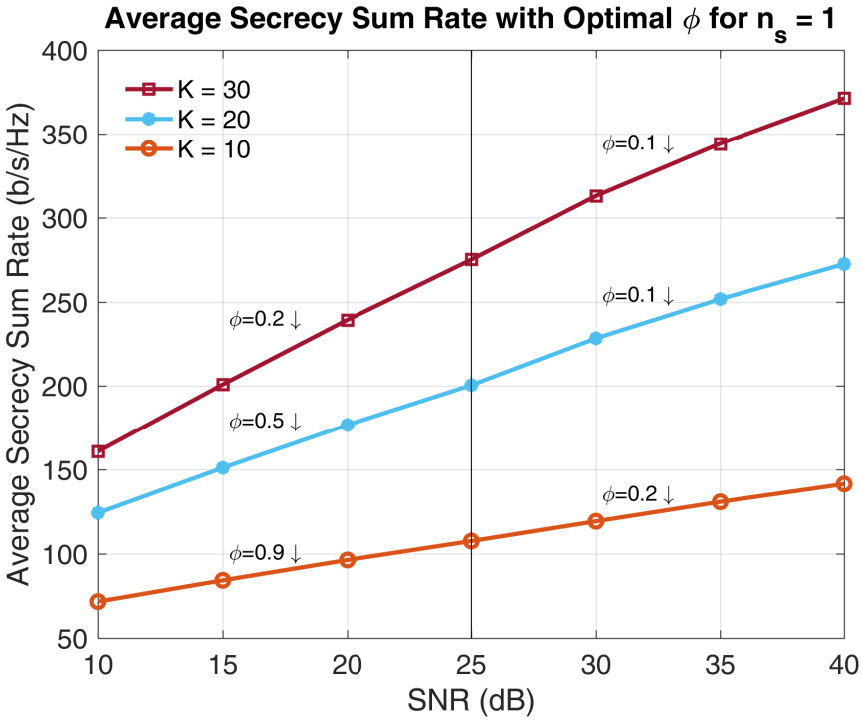

Figure 3.9. Average secrecy sum rate vs SNR and K for $n_s = 1$.

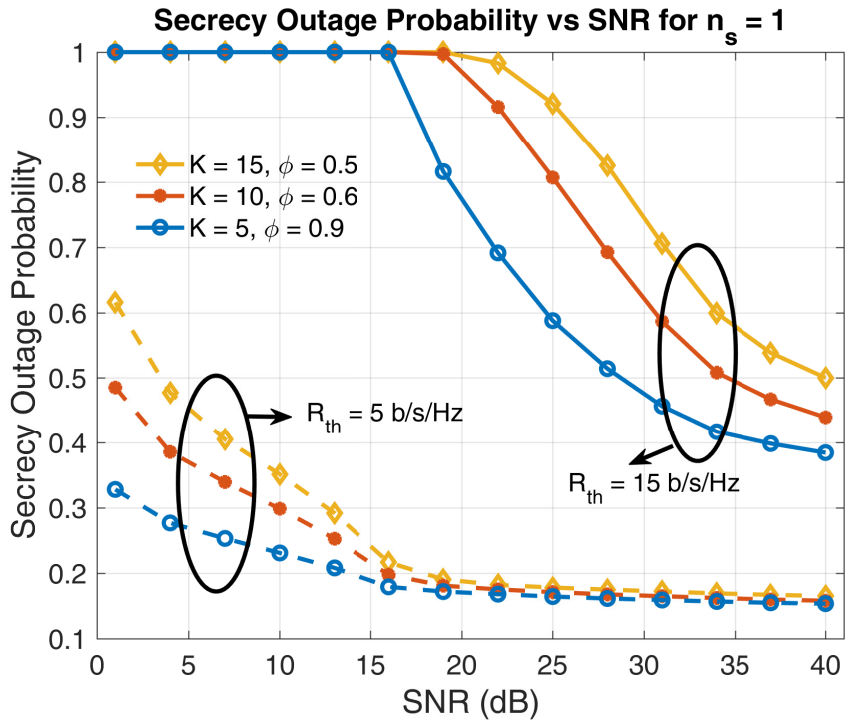

Figure 3.10. Secrecy outage probability vs SNR for K and $n_s = 1$ with optimum ϕ.

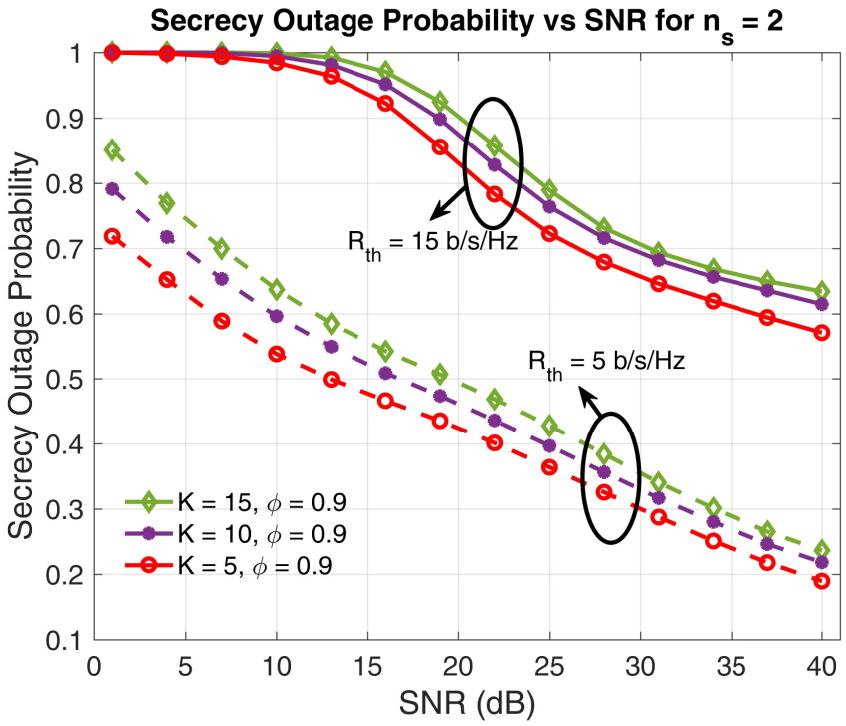

Figure 3.11. Secrecy outage probability vs SNR and K for $n_s = 2$ with optimum $\phi = 0.9$.

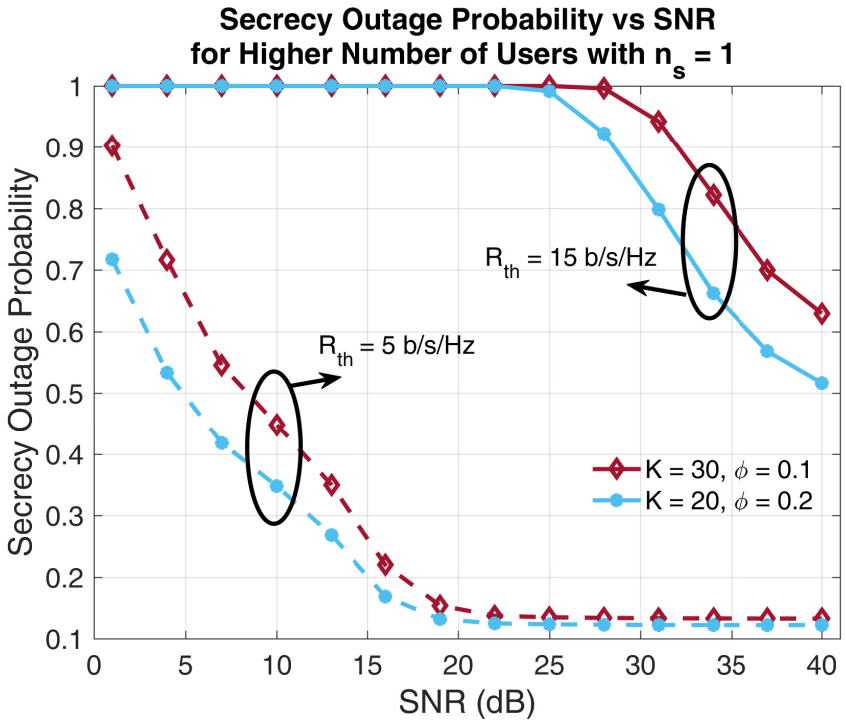

Figure 3.12. Secrecy outage probability vs SNR and K for $n_s = 1$ with optimum ϕ.

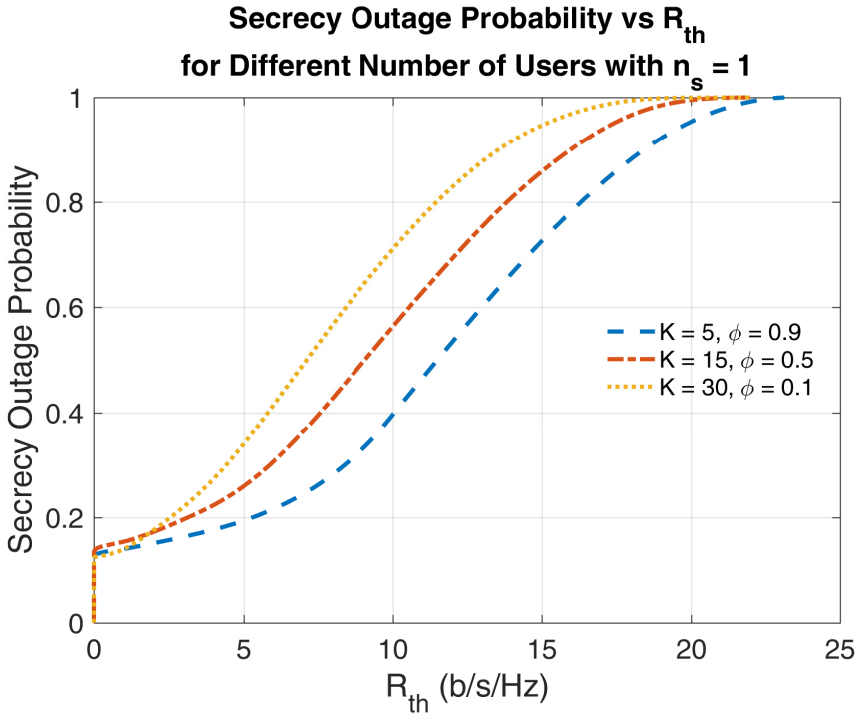

Figure 3.13. Secrecy outage probability vs R_{th} and K for $n_s = 1$ with optimum ϕ.

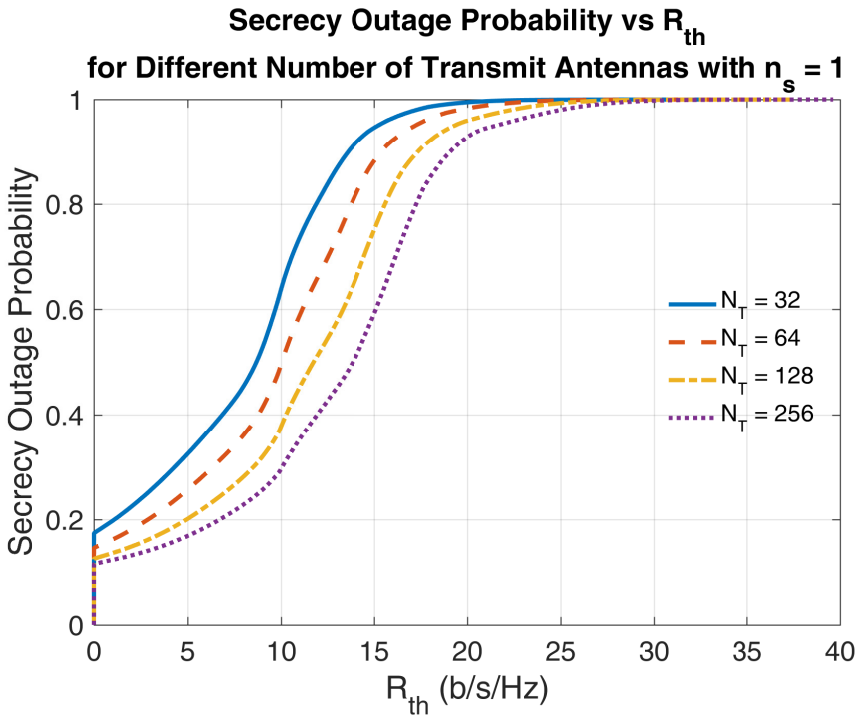

Figure 3.14. Secrecy outage probability vs R_{th} and N_T for K = 30 and $n_s = 1$.

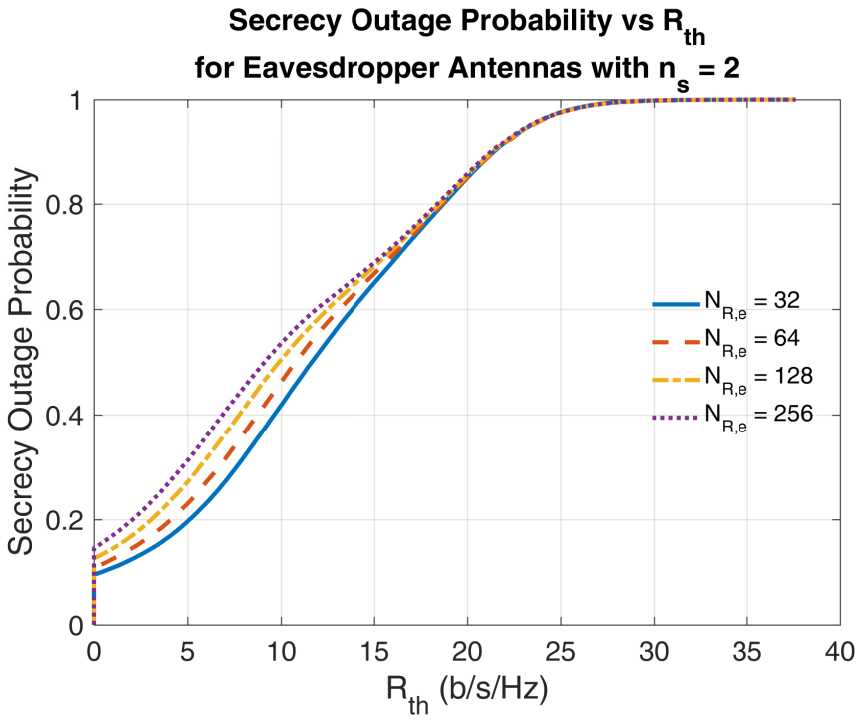

Figure 3.15. Secrecy outage probability vs R_{th} and $N_{R,e}$ for K = 30 $n_s = 2$.

CHAPTER 4

SECURE MULTICELL MULTIUSER MIMO SYSTEMS

In this chapter, we extend our system to the secure multicell mmWave MU-MIMO communications (Erdoğan and Özbek, 2020). Firstly, we give related works in the literature. Secondly, we define a secure multicellular mmWave communication scenario. Thirdly, we xplaine the hybrid MIMO beamforming techniques in coordinated and non-coordinated points of view. Finally, we provide the simulation results for the secure multicell mmWave MU-MIMO system.

4.1. Related Works

Focusing on the PLS, a lot of diverse scenarios have been investigated by the researchers recently. The authors in (Sadeghzadeh et al., 2018),(Ng et al., 2014),(Zhu et al., 2014) have considered the PLS for the sub-6GHz channel while authors in (Ju et al., 2017),(Wang et al., 2019), and (Lin et al., 2017) have analyzed the PLS for the mmWave channel. In (Sadeghzadeh et al., 2018), the MU-MIMO communication with different precoders based on the ZF and MMSE techniques have been considered in the presence of a passive eavesdropper. However, the asymptotic secrecy sum rate has been provided under the imperfect CSI. The robust beamforming has been proposed in (Ng et al., 2014) by solving the resource allocation problem for the multiuser multiple-input single-output (MISO) wireless information and power transfer system. Nonetheless, AN and MRT precoders for the multicell MU-MIMO have been studied by considering the secrecy rate and the secrecy outage probability in (Zhu et al., 2014).

In (Ju et al., 2017), the PLS for the mmWave channels has been studied for the multiuser MISO systems while it has also studied for the MU-MIMO with two-stage relay systems via hybrid beamforming architecture in (Wang et al., 2019). On the other hand, a different approach has been proposed in (Lin et al., 2017) in which the frequency offset across antenna arrays can be adjusted well if the channel of each user is becoming correlated. This method is called the frequency diverse array beamforming but this concept

is out of scope for this thesis. As a consequence, we have extended these studies to the multicell MU-MIMO mmWave communication systems by applying PLS techniques.

The secure communication for the mmWave multicell MU-MIMO scenario is investigated. By comparing the different beamforming techniques, we assume that there is only one eavesdropper that is similar to the previous chapter and it can receive the messages from the channel of each legitimate user by sharing the same AoDs. The eavesdropper behaves as a passive receiver that hides its presence and its CSI as well. Thus, we apply AN beamforming to enhance the security of the system. Our contributions can be summarized as followings:

1. Considering the 3D mmWave channel model, we provide a multicell scenario for the MU-MIMO by taking into account the PLS, achievable data rate, and so forth. While the hybrid beamforming scheme is employed at the BSs, users, and eavesdropper, we present how the analog and digital beamformers can be successfully obtained.

2. We present a comprehensive study about different linear precoding techniques that are divided into two subgroups namely CoMP and non-CoMP. We consider MRT, ZF, and random beamformer (RB) precoders for the non-CoMP case whereas the signal to leakage plus noise ratio (SLNR) based precoder is considered for the CoMP case. Moreover, we compare them according to spectral efficiency, security, and the computational complexity.

3. We examine the PLS for the multicell mmWave MU-MIMO communication network. Furthermore, we take into consideration the secrecy rate and we observe the secrecy outage probability with a given threshold rate. Finally, we employ AN in order to ensure security and observing the advantages and disadvantages of it on the system.

4.2. System Model

The system deployment is depicted in Figure (4.1). In this system, we assume that the frequency reuse factor is equal to 1 which means all BSs operate the same frequency.

Each cell in Figure (4.1) has its own BS and the total number of BSs is J. Moreover, each BS is equipped with N_T antennas and N_{RF} chains. On the opposite, we assume that there are K total number of legitimate users in the system, G is the number of legitimate users in the jth BS, and each user is equipped with N_R antennas and M_{RF} RF chains that satisfies $N_{RF} >> M_{RF}$ for more realistic and practizable scenario. Consequently, all BSs and legitimate users are employed to hybrid beamforming scheme which is highly suitable and efficient for the large antenna system scenarios and mmWave communications. We focus on the multicell, MU-MIMO scenario where the eavesdropper can access some AoDs of legitimate users as similar in Section 3.2.

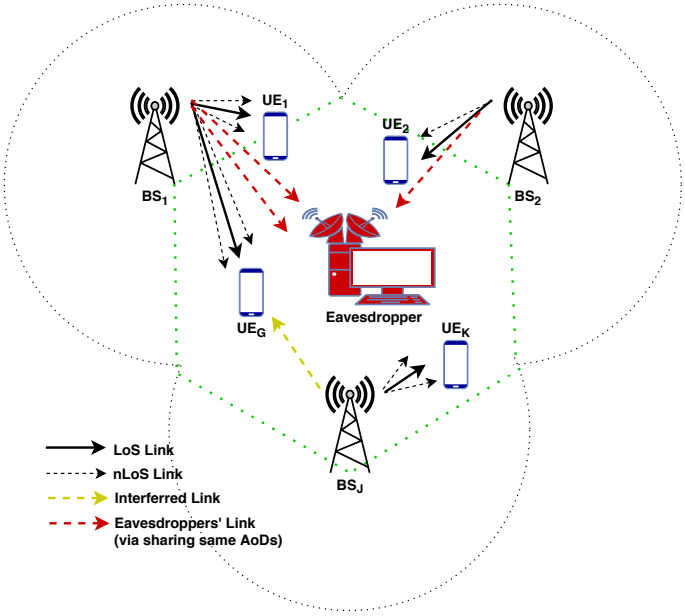

Figure 4.1. Secure mmWave multicell MU-MIMO downlink communications.

4.3. The Proposed Scheme

We propose a secure multiuser multicell mmWave system employing hybrid beamforming as shown in Figure (4.2). The digital precoder at the jth BS is defined by $\mathbf{F}^j_{DB} \in \mathbb{C}^{N_{RF} \times N_s}$ while the analog precoder is defined by $\mathbf{F}^j_{AB} \in \mathbb{C}^{N_T \times N_{RF}}$ where N_s indicate the total number of streams sent from the single BS to G number of legitimate users. On the other side, the digital combiner and the analog combiner for the gth legitimate user in the jth BS are defined by $\mathbf{W}^j_{DB,g} \in \mathbb{C}^{M_{RF} \times n_s}$ and $\mathbf{W}^j_{AB,g} \in \mathbb{C}^{N_R \times M_{RF}}$, respectively. The number of data stream per user is denoted by n_s.

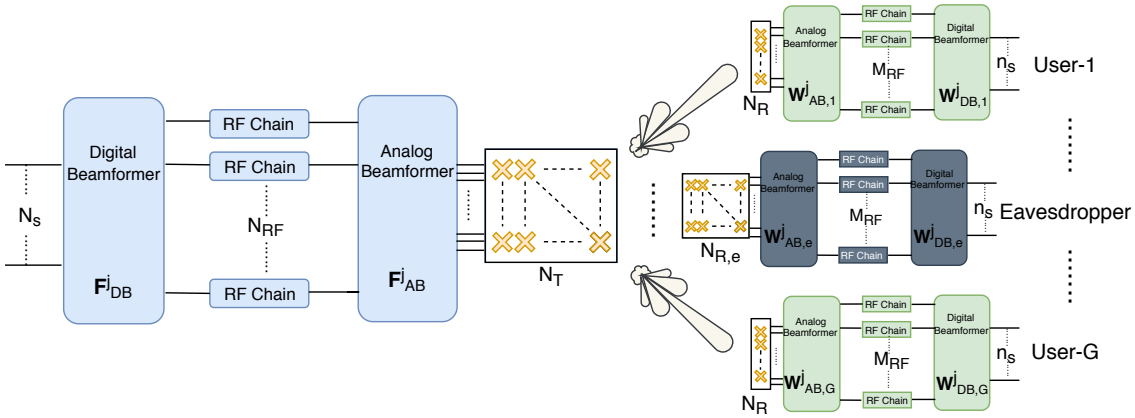

Figure 4.2. Hybrid ccheme at BS, legitimate users, and eavesdroppers in the *j*th cell.

Using hybrid architecture, the transmit signal $\widetilde{\mathbf{x}}^j \in \mathbb{C}^{N_T \times 1}$ at the *j*th BS which is similar to Eq.(3.1) can be defined as,

$$\widetilde{\mathbf{x}}^j = \sqrt{\phi^j}\mathbf{F}^j_{AB}\mathbf{F}^j_{DB}\mathbf{s}^j + \sqrt{1-\phi^j}\mathbf{F}^j_{AN}\mathbf{z}^j \tag{4.1}$$

where $\mathbf{F}^j_{AB} = \left[\mathbf{F}^j_{AB,1}, \ldots, \mathbf{F}^j_{AB,g}, \ldots, \mathbf{F}^j_{AB,G}\right]$ and $\mathbf{F}^j_{DB} = \left[\mathbf{F}^j_{DB,1}, \ldots, \mathbf{F}^j_{DB,g}, \ldots, \mathbf{F}^j_{DB,G}\right]$ are the concatenated analog and digital precoders, respectively. ϕ^j is denoted as the power allocation factor between the precoders of legitimate users and AN. The AN precoder, $\mathbf{F}^j_{AN} \in \mathbb{C}^{N_T \times (N_s - GM_{RF})}$ can be obtained from Eq.(3.5) for each BS.

Furthemore, the received signal by the *k*th legitimate user out of *K* legitimate users from the *j*th BS out of *J* BSs can be defined as,

$$\begin{aligned}
\mathbf{y}^j_k = &\sqrt{\phi^j P^j_k}(\mathbf{W}^j_{DB,k})^H(\mathbf{W}^j_{AB,k})^H\mathbf{H}^j_k\mathbf{F}^j_{AB,k}\mathbf{F}^j_{DB,k}\mathbf{s}^j_k \\
&+ \sum_{\substack{g\neq k \\ g=1}}^{G}\sqrt{\phi^j P^j_k}(\mathbf{W}^j_{DB,k})^H(\mathbf{W}^j_{AB,k})^H\mathbf{H}^j_k\mathbf{F}^j_{AB,g}\mathbf{F}^j_{DB,g}\mathbf{s}^j_g \\
&+ \sum_{\substack{i\neq j \\ i=1}}^{J}\sum_{n=1}^{G}\sqrt{\phi^j P^i_n}(\mathbf{W}^j_{DB,k})^H(\mathbf{W}^j_{AB,k})^H\mathbf{H}^i_k\mathbf{F}^i_{AB,n}\mathbf{F}^i_{DB,n}\mathbf{s}^i_n \\
&+ \sqrt{(1-\phi^j)P^j_k}(\mathbf{W}^j_{DB,k})^H(\mathbf{W}^j_{AB,k})^H\mathbf{H}^j_k\mathbf{F}^j_{AN}\mathbf{z}^j \\
&+ (\mathbf{W}^j_{DB,k})^H(\mathbf{W}^j_{AB,k})^H\mathbf{n}^j_k
\end{aligned} \tag{4.2}$$

where P_k^j is the received power for the *k*th user at the *j*th BS. The first line is the desired signal, the second and the third line denote the intra-cell interference and the inter-cell interference, respectively. While the fourth line indicates the AN beamforming, the fifth line indicates the noise. The channel matrix for the kth legitimate user in the jth BS is denoted by $\mathbf{H}_k^j \in \mathbb{C}^{N_R \times N_T}$ and it can be obtained by using the Eq.(2.1). $\mathbf{n}_k^j$ is the complex AWGN whose elements are zero mean and σ_k^2 variance $\mathcal{CN}(0, \sigma_k^2)$. Nevertheless, the received signal by the corresponding eavesdropper is defined as,

$$\begin{aligned}\mathbf{y}_{e,k}^j = &\sqrt{\phi^j P_k^j}(\mathbf{W}_{DB,e,k}^j)^H(\mathbf{W}_{AB,e,k}^j)^H\mathbf{H}_{e,k}^j\mathbf{F}_{AB,k}^j\mathbf{F}_{DB,k}^j\mathbf{s}_k^j \\ &+ \sqrt{(1-\phi^j)P_k^j}(\mathbf{W}_{DB,e,k}^j)^H(\mathbf{W}_{AB,e,k}^j)^H\mathbf{H}_{e,k}^j\mathbf{F}_{AN}^j\mathbf{z}^j \\ &+ (\mathbf{W}_{DB,e,k}^j)^H(\mathbf{W}_{AB,e,k}^j)^H\mathbf{n}_{e,k}^j\end{aligned} \tag{4.3}$$

where the first row is the intended signal traveling to the desired legitimate user. The eavesdropper tries to obtain the message signal perfectly. However, the second row is the AN signal that provides to disrupt the eavesdropper channel. The last row indicates the noise signal. We assume that the eavesdropper can only receive the message signal and AN signal since it is able to cancel out the interfered signals as distinct from the received signals by the legitimate users given in Eq.(4.3).

In both Eq.(4.2) and Eq.(4.3), the analog precoder and combiner matrices for the each legitimate user and the corresponding eavesdropper in the *j*th BS can be obtained from Algorithm 1 in Section 2. Similarly in Eq.(2.19), the effective channel matrix for the *k*th legitimate user in the *j*th BS is calculated as,

$$\mathbf{H}_{eff,k}^j = (\mathbf{W}_{AB,k}^j)^H\mathbf{H}_k^j\mathbf{F}_{AB,k}^j \tag{4.4}$$

After defining the effective channel, the next step is to design the digital precoders using the effective channel matrix for each legitimate user. The digital combiner for the *k*th legitimate user in the *j*th BS, $\mathbf{W}_{DB,k}^j$ are chosen as MRC that can be obtained by employing the Eq.(2.27) with a similar way. Furthermore, the digital combiner of the corresponding eavesdropper, $\mathbf{W}_{DB,e,k}^j$ can be calculated as,

$$\mathbf{W}^{j}_{DB,e,k} = \frac{(\mathbf{W}^{j}_{AB,e,k})^{H}\mathbf{H}^{j}_{e,k}\mathbf{F}^{j}_{AB,k}\mathbf{F}^{j}_{DB,k}}{||(\mathbf{W}^{j}_{AB,e,k})^{H}\mathbf{H}^{j}_{e,k}\mathbf{F}^{j}_{AB,k}\mathbf{F}^{j}_{DB,k}||_{F}} \tag{4.5}$$

Before introducing the multicell digital precoding techniques, we define the SINR of each legitimate user and corresponding eavesdropper as,

$$\begin{aligned}\boldsymbol{\gamma}^{j}_{k} =&(\mathbf{D}^{j}_{k} + \mathbf{D}^{j}_{AN,k} + \mathbf{R}^{j}_{kk})^{-1} \\ &(\mathbf{W}^{j}_{DB,k})^{H}(\mathbf{W}^{j}_{AB,k})^{H}\mathbf{H}^{j}_{k}\mathbf{F}^{j}_{AB,k}\mathbf{F}^{j}_{DB,k}(\mathbf{F}^{j}_{DB,k})^{H}(\mathbf{F}^{j}_{AB,k})^{H}(\mathbf{H}^{j}_{k})^{H}\mathbf{W}^{j}_{AB,k}\mathbf{W}^{j}_{DB,k}\end{aligned} \tag{4.6}$$

where $\boldsymbol{\gamma}^{j}_{k}$ stands for the SINR of the *k*th legitimate user in the *j*th BS and $\mathbf{D}^{j}_{k}$ is the interference matrix for the *k*th legitimate user at the *j*th BS that is defined as,

$$\begin{aligned}\mathbf{D}^{j}_{k} = (\mathbf{W}^{j}_{DB,k})^{H}(\mathbf{W}^{j}_{AB,k})^{H} \Bigg(&\sum_{\substack{g\neq k \\ g=1}}^{G} \mathbf{H}^{j}_{k}\mathbf{F}^{j}_{AB,g}\mathbf{F}^{j}_{DB,g}(\mathbf{F}^{j}_{DB,g})^{H}(\mathbf{F}^{j}_{AB,g})^{H}(\mathbf{H}^{j}_{k})^{H} \\ &+ \sum_{\substack{i\neq j \\ i=1}}^{J}\sum_{n=1}^{G} \mathbf{H}^{i}_{k}\mathbf{F}^{i}_{AB,n}\mathbf{F}^{i}_{DB,n}(\mathbf{F}^{i}_{DB,n})^{H}(\mathbf{F}^{i}_{AB,n})^{H}(\mathbf{H}^{i}_{k})^{H} \Bigg) \mathbf{W}^{j}_{AB,k}\mathbf{W}^{j}_{DB,k}\end{aligned} \tag{4.7}$$

where $\mathbf{D}^{j}_{AN,k}$ in the Eq.(4.6) is the AN precoder which propagates from the *j*th BS through the *k*th legitimate user can be defined as,

$$\mathbf{D}^{j}_{AN,k} = (\mathbf{W}^{j}_{DB,k})^{H}(\mathbf{W}^{j}_{AB,k})^{H}\mathbf{H}^{j}_{k}\mathbf{F}^{j}_{AN}(\mathbf{F}^{j}_{AN})^{H}(\mathbf{H}^{j}_{k})^{H}\mathbf{W}^{j}_{AB,k}\mathbf{W}^{j}_{DB,k} \tag{4.8}$$

and where $\mathbf{R}^{j}_{kk}$ in the Eq.(4.6) is the noise covariance matrix for the *k*th legitimate user in the *j*th BS is evaluated as,

$$\mathbf{R}^{j}_{kk} = (\mathbf{W}^{j}_{DB,k})^{H}(\mathbf{W}^{j}_{AB,k})^{H}\mathbf{W}^{j}_{AB,k}\mathbf{W}^{j}_{DB,k} \tag{4.9}$$

Similarly, the SINR of corresponding eavesdropper for the *k*th legitimate user in the *j*th BS can be obtained by using Eq.(4.5) as,

$$\boldsymbol{\gamma}^{j}_{e,k} = (\mathbf{D}^{j}_{AN,e,k} + \mathbf{R}^{j}_{ee,kk})^{-1} \\ (\mathbf{W}^{j}_{DB,e,k})^{H}(\mathbf{W}^{j}_{AB,e,k})^{H}\mathbf{H}^{j}_{e,k}\mathbf{F}^{j}_{AB,k}\mathbf{F}^{j}_{DB,k}(\mathbf{F}^{j}_{DB,k})^{H}(\mathbf{F}^{j}_{AB,k})^{H}(\mathbf{H}^{j}_{e,k})^{H}\mathbf{W}^{j}_{AB,e,k}\mathbf{W}^{j}_{DB,e,k} \tag{4.10}$$

where $\mathbf{D}^{j}_{AN,k}$ is the AN precoder which propagates from the *j*th BS through the eavesdropper is defined as,

$$\mathbf{D}^{j}_{AN,e,k} = (\mathbf{W}^{j}_{DB,e,k})^{H}(\mathbf{W}^{j}_{AB,e,k})^{H}\mathbf{H}^{j}_{e,k}\mathbf{F}^{j}_{AN}(\mathbf{F}^{j}_{AN})^{H}(\mathbf{H}^{j}_{e,k})^{H}\mathbf{W}^{j}_{AB,e,k}\mathbf{W}^{j}_{DB,e,k} \tag{4.11}$$

and where $\mathbf{R}^{j}_{ee,kk}$ in the Eq.(4.10) is the noise covariance matrix of corresponding eavesdropper for the *k*th legitimate user in the *j*th BS is defined as,

$$\mathbf{R}^{j}_{ee,kk} = (\mathbf{W}^{j}_{DB,e,k})^{H}(\mathbf{W}^{j}_{AB,e,k})^{H}\mathbf{W}^{j}_{AB,e,k}\mathbf{W}^{j}_{DB,e,k} \tag{4.12}$$

After that, the data rate of the *k*th legitimate user in the *j*th BS can be calculated as,

$$R^{j}_{k} = \log_2 \left|\mathbf{I}_{n_s} + \boldsymbol{\gamma}^{j}_{k}\right| \tag{4.13}$$

The corresponding eavesdropper's data rate can be given as,

$$R^{j}_{e,k} = \log_2 \left|\mathbf{I}_{n_s} + \boldsymbol{\gamma}^{j}_{e,k}\right| \tag{4.14}$$

Finally, the average secrecy rate for the *k*th legitimate user in the *j*th BS is defined by,

$$R^{j}_{s,k} = \mathbb{E}\{[R^{j}_{k} - R^{j}_{e,k}]^{+}\} \tag{4.15}$$

where $R_{s,k}^{j}$ is the average secrecy rate of the *k*th legitimate user in the *j*th BS and $[x]^{+} \triangleq \max\{0, x\}$. The average secrecy sum rate in the multicell is given as,

$$R_s = \sum_{j=1}^{J} \sum_{g=1}^{G} R_{s,g}^{j} \tag{4.16}$$

The secrecy outage probability is obtained through the Eq.(3.14) by using Eq.(4.15).

4.4. Multicell MIMO Precoding Techniques

Since we consider the multiple streams and MU-MIMO communication, we must choose the appropriate precoding methods to serve multiple users with multiple streams simultaneously. Before we introduce the digital precoding methods for the multi cellular systems, we first divide the digital precoder methods into two categories; as the non-coordinated (non-CoMP) and coordinated (CoMP) methods (Sun et al., 2018). We consider the MRT, ZF, and the RB (Lee et al., 2016),(Vicario et al., 2008),(Chung et al., 2003) precoders (RB is not a new method, however, it is the first time that it is investigated for the mmWave systems) for the non-coordinated cases. For the coordinated cases, the SLNR based precoding is considered. We will further explain the RB precoders in the next sections.

Choosing as the number of data streams per user (n_s) equal to the number of RF chains at users (M_{RF}) makes the calculations easier. Since we select $n_s = M_{RF}$, we just need M_{RF} RF chains out of N_{RF} RF chains at the BSs for each user. Similarly, we only need n_s streams out of N_s streams at the BSs for each user. Thus, the analog and digital precoder for the *k*th user in the *j*th BS should be at the dimensions of $N_T \times M_{RF}$ and $M_{RF} \times n_s$, respectively.

4.4.1. SLNR Based Precoding (CoMP)

The first explored multicell MIMO precoding technique is the SLNR based precoding that maximizes the signal to leakage plus noise ratio (SLNR). In this case, we

assume that there is coordination among the BSs so that all BSs share the CSI of their users with each other. Because of the optimal power allocation for a large number of users is a challenging problem, SLNR based precoder with CoMP does not need for an optimal power allocation scheme since it mitigates interference and gives the best beamformer to each user (Sun et al., 2018). For the SLNR based precoder, we first define a new effective channel matrix regarding to leakage for the kth user in the jth BS such that

$$\mathbf{H}_{eff,m,k}^{i,j} = \mathbf{W}_{AB,m}^{i}\mathbf{H}_{m}^{i}\mathbf{F}_{AB,k}^{j} \tag{4.17}$$

where $i = 1, \ldots, J$ with $(i = j)$, and $m = 1, \ldots, G$ with $(m \neq k)$.

Then the leakage matrix $(K-1)M_{RF} \times M_{RF}$ for the kth user in the *j*th BS can be derived as (Sun et al., 2018),

$$\dot{\mathbf{H}}_{k}^{j} = [(\mathbf{H}_{eff,1,k}^{1,j})^{T}, \ldots, (\mathbf{H}_{eff,m-1,k}^{i,j})^{T}, (\mathbf{H}_{eff,m+1,k}^{i,j})^{T}, \ldots, (\mathbf{H}_{eff,(K-1),k}^{J,j})^{T}]^{T} \tag{4.18}$$

Since $\mathbb{E}[\mathbf{s}_{k}^{j}(\mathbf{s}_{k}^{j})^{H}] = \mathbf{I}_{n_s}$ and $\mathbb{E}[\mathbf{n}_{k}^{j}(\mathbf{n}_{k}^{j})^{H}] = \sigma_{k}^{2}\mathbf{I}_{N_R}$, the normalization factor ζ can be given as (Sun et al., 2018),

$$\zeta = \frac{\sigma_{k}^{2}}{P_{k}^{j}}\text{tr}(\mathbf{W}_{AB,k}^{j}(\mathbf{W}_{AB,k}^{j})^{H}) \tag{4.19}$$

Finally, the digital precoder for the *k*th user in the *j*th BS can be calculated by using (4.4) and (4.18) (Sadek et al., 2007) as,

$$\bar{\mathbf{U}}\bar{\mathbf{\Sigma}}\bar{\mathbf{V}}^{*} = \left(\zeta\mathbf{I}_{M_{RF}} + (\dot{\mathbf{H}}_{k}^{j})^{H}\dot{\mathbf{H}}_{k}^{j}\right)^{-1}(\mathbf{H}_{eff,k}^{j})^{H}\mathbf{H}_{eff,k}^{j} \tag{4.20}$$

$$\mathbf{F}_{DB,k}^{j} = \bar{\mathbf{V}}_{(:,1:n_s)} \tag{4.21}$$

where $\mathbf{F}^{j}_{DB,k}$ and the digital precoder of each user should be normalized by its analog counterpart to satisfy the transmit power constraint, $||\mathbf{F}^{j}_{AB,k}\mathbf{F}^{j}_{DB,k}||^2_F = 1$, such as,

$$\mathbf{F}^{j}_{DB,k} = \frac{\mathbf{F}^{j}_{DB,k}}{||\mathbf{F}^{j}_{AB,k}\mathbf{F}^{j}_{DB,k}||_F} \tag{4.22}$$

4.4.2. MRT Precoding (non-CoMP)

Without using any BS coordination, we first examine the MRT precoding technique. In this case, we first define $GM_{RF} \times M_{RF}$ concatenated effective channel matrix for the *j*th BS as (Sun et al., 2018),

$$\bar{\mathbf{H}}_j = [(\mathbf{H}^{j}_{eff,1})^T, \ldots, (\mathbf{H}^{j}_{eff,k})^T, \ldots, (\mathbf{H}^{j}_{eff,G})^T]^T \tag{4.23}$$

Furthermore, the $M_{RF} \times GM_{RF}$ generalized MRT precoding matrix for the jth BS can be obtained as (Sun et al., 2018),

$$\mathbf{F}^{j}_{DB} = \bar{\mathbf{H}}^{H}_{j} \tag{4.24}$$

where $\mathbf{F}^{j}_{DB} = [\mathbf{F}^{j}_{DB,1} \ldots \mathbf{F}^{j}_{DB,k} \ldots \mathbf{F}^{j}_{DB,G}]$. Equivalently, MRT precoder of the each user can be obtained by,

$$\mathbf{F}^{j}_{DB,k} = (\mathbf{H}^{j}_{eff,k})^{H} \tag{4.25}$$

Finally, MRT precoder for each user must satisfy the transmit power constraint by using Eq.(4.22).

4.4.3. ZF Precoding (non-CoMP)

In the non-CoMP case, another most commonly used precoding method is the ZF due to it mitigates the multiuser interference. Using (4.23), the $M_{RF} \times GM_{RF}$ ZF precoding for the *k*th user in the *j*th BS can be defined as,

$$\mathbf{F}_{DB}^{j} = \bar{\mathbf{H}}_{j}^{H}(\bar{\mathbf{H}}_{j}\bar{\mathbf{H}}_{j}^{H})^{-1} \tag{4.26}$$

ZF precoder for each user must satisfy the transmit power constraint so that Eq.(4.22) should be used.

4.4.4. RB Precoding (non-CoMP)

The random beamforming method has been proposed by Chung in (Chung et al., 2003) for the MIMO communications. The main idea is to find the most suitable beamformer by using random beamformer generator that maximize the effective SNR (ESNR) of users. According to the feedback of users, the best beamformer is selected for each user. In (Vicario et al., 2008) the orthogonal random beamforming and beam selection strategies has been examined. Here after, the random beamforming has also been studied in (Lee et al., 2016) on the sparse mmWave channels. Nevertheless, there are many studies about random beamforming in literature but we are going to deal with a different approach in this thesis.

Assuming each BS has its own storage or memory to keep their beamformers and they are able to generate their beamformers randomly. Using proper scheduling, we can assign different beamformers to different users.

Firstly, we define a set of N_{pre} candidate precoding vectors is given as,

$$\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_{N_{pre}}\} \tag{4.27}$$

where each precoder i.e., $\mathbf{b}_r$ is a normally distributed complex vector with zero mean and σ_r^2 variance such that $\mathbf{b}_r \sim C\mathcal{N}(0, \sigma_r^2)$ with the dimension of $M_{RF} \times 1$. Regardless of using any scheduling algorithm, we select the most suitable n_s precoding vectors that maximize the Euclidean norm of the corresponding effective channel matrix of each user by doing exhaustive searching on the set of available precoders. For the kth user in the jth BS, the digital precoder can be obtained as,

$$\mathbf{F}_{DB,k}^{j} = \left[\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_{n_s}^*\right]$$
$$\text{where} \quad \mathbf{b}_n^* = \max_{r=1,\ldots,N_{pre}} ||\mathbf{H}_{eff,k}^{j}\mathbf{b}_r||^2, \qquad n = 1, ..., n_s \tag{4.28}$$

where $\mathbf{F}_{DB,k}^{j}$ should be normalized by Eq.(4.22) to satisfy the transmit power constraint.

Using random precoders can provide more effective transmission at the BS side because all streams that belongs to each user can be well constructed. In addition, any scheduling method will be out of scope for this thesis except in Eq.(**??**). However, this method starts from the first user and it gives the best precoder vector to it rather than giving the optimal one. This may not be fair for other users. Thus, this method needs a fair or an appropriate scheduling for further improvement.

4.4.5. Complexity Analysis

Table 4.1. Computational Complexity of Beamforming Methods

Beamforming	Operation	*flops*	$K = 100$ $n_s = 2$ $N_{pre} = 5Kn_s$
ZF	$(\bar{\mathbf{H}}_k^j)^H(\bar{\mathbf{H}}_k^j(\bar{\mathbf{H}}_k^j)^H)^{-1}$	$J[16(Gn_s)^3 - 10(Gn_s)^2 + 8(Gn_s)^2n_s + 8(Gn_s)n_s^2$ $+2(Gn_s) - 2(Gn_s)n_s]$	13.8×10^6
SLNR-CoMP	$svd[(\zeta\mathbf{I}_{n_s} + (\dot{\mathbf{H}}_k^j)^H\dot{\mathbf{H}}_k^j)^{-1}(\mathbf{H}_{eff,k}^j)^H\mathbf{H}_{eff,k}^j]$	$K[16(Ln_s)^3 - 10(Ln_s)^2 + 8(Ln_s)^2n_s + 8(Ln_s)n_s^2 + 4(Ln_s)]$ $+8K[21(n_s)^3]$	12.4×10^9
RB	$\arg\max_{n_s} \max_{r=1,\ldots,N_{pre}} ||\mathbf{H}_{eff,k}^j\mathbf{b}_r^*||^2$	$J[Gn_sN_{pre}(2n_s^2 + 2n_s)]$	2.4×10^6

The computational complexity is a crucial metric for many real-time applications. Thus, we need to take into account the complexity of the different beamforming methods

that we examine in this section. To determine how an algorithm or any computation is counted as a complexity measure, we generally use *flops* which is floating point defined in (Golub and Van Loan, 2012). The flops calculation for ZF precoder and the SVD computation are described in (Sadeghzadeh et al., 2018). We further extend this study to flops computation for SLNR based precoder. We also compute the flops for RB by using frobenius norm which is described in (Shen et al., 2006).

The required flops calculation for the different precoder techniques are given in Table 4.1. By using the following parameters; the number of BSs as $J = 3$, the average number of users in each BS as $G = K/J$ where K is the total number of users and the average number of users for the leakage as $L = (K-1)/(J/3)$ where the number 3 is used for three sectorized multicell deployments. In the Table 4.1, the CoMP based precoder is more computationally complex than non-CoMP precoders. Nonetheless, the CoMP based SLNR precoder is getting more computationally heavy when the system becomes large. In other words, if the BSs or users need multiple streams or the network has more BSs and/or users, SLNR based precoder is not so efficient even if it provides the best sum rate performance. Furthermore, ZF precoder is also computationally complex since it needs to take an inverse operation on the concatenated effective channel matrix. On the other side, MRT is the simplest precoder among all precoders but it cannot mitigate the interference. Thus, RB precoder can be selected as a good alternative for such systems.

4.5. Performance Evaluations

In this section, we provide the simulation results to illustrate the system performance in terms of the sum data rate, the secrecy sum rate and the secrecy outage probability. The important simulation parameters are given in Table 4.2 and the mmWave channel parameters are given in Table 2.1. We assume that RB precoders for each BS are initially generated and stored in a memory to reduce computational complexity given in Table 4.1. Finally, the results are obtained by the Monte Carlo simulations.

Since security is the main consideration for this thesis, following Figures (4.3) - (4.10) represent the power allocation factor between different precoder techniques and AN precoder. We employ different precoders at the BSs to observe their effects on the system consisting of both K = 45 or K = 90 legitimate users. The power allocation value is

determined for each precoder uniquely. For example, the SLNR gives better performance for both K = 45 and K = 90 when $n_s = 2$. It is also noted that giving less power to MRT and more power to AN can enhance the secrecy since MRT improves the data rate performance, especially in the low SNR region.

Table 4.2. Simulation Parameters for Secure Multi Cell mmWave MU-MIMO Systems

Parameter	**Description**	**Value**
N_T	Number of antennas at BSs	256
N_R	Number of antennas at Legitimate Users	16
$N_{R,e}$	Number of antennas at Eavesdroppers	64
J	Total number of BSs	3
K	Total number of users	[45,90]
G	Number of users in each BS	K/J
N_{pre}	Number of available random precoders	$5Kn_s$
n_s	Number of data streams for each user	[1,2]
N_s	Number of data streams for BS	Gn_s
M_{RF}	Number of RF chains at users	n_s
N_{RF}	Number of RF chains at BSs	64

In Figure (4.11), the average sum data rate is drawn to show the comparison of different beamforming techniques both for $K = 45$ and $K = 90$ legitimate users using $n_s = 2$ without considering secrecy. The SLNR precoder gives the best sum data rate performance while MRT is the worst one. The CoMP based SLNR utilizes the coordination of BSs to prevent information leakage. However, MRT can not mitigate this information leakage. It is also worth noting that RB precoders outperform MRT and they give the same results as much as ZF.

The average secrecy sum rate is drawn for two different number of users and different precoding techniques with their optimum power allocation values in Figure (4.12). The secrecy sum rate enhances as the number of users increases. While SLNR performs the best secrecy sum rate performance at the high SNR region, MRT gives the best performance at the low SNR region for both cases. When using the large antenna arrays at the BSs, MRT can be considered for the proper precoder to satisfy the secrecy requirements for the mmWave communication. Even though RB performs the same secrecy rate as ZF, ZF is getting better than RB for the user densities becomes larger. Thus, RB needs the novel algorithms and/or new strategies to fair scheduling for further improvements.

Figures (4.13) and (4.14) draw the secrecy outage probability with respect to SNR for two different threshold rates and different number of precoders considering their optimal power allocation values determined by Figures (4.4)-(4.7). MRT precoder improves secrecy outage at the low threshold rate but it also performs worse at the high threshold rate. It can be explained that MRT directly depends on the channel conditions, and if the channel is poor, MRT gives also poor performance or vice versa. Also, SLNR precoder gives the best performance for the higher threshold rates.

The computational complexity is given for each precoder technique including ZF, SLNR, and RB in Figure (4.15). SLNR has the highest complexity even if it gives the best performance in terms of data rate and secrecy. However, RB precoder is the second non-complex technique after MRT. Since MRT is the simplest precoder among all precoder techniques, it does not need any effort for computation. On the other hand, the computational complexity of ZF is getting high when the number of users increases. Hence, RB provides almost the same performance with ZF while having less complexity for the MU-MIMO mmWave communication systems. It can be a good alternative for these systems instead of other well-known precoding techniques.

As a summary, we have examined different precoding techniques for the secure multicell mmWave scenario. The importance of secrecy, complexity and latency, quality of service (QoS) requirements may vary from applications to applications.

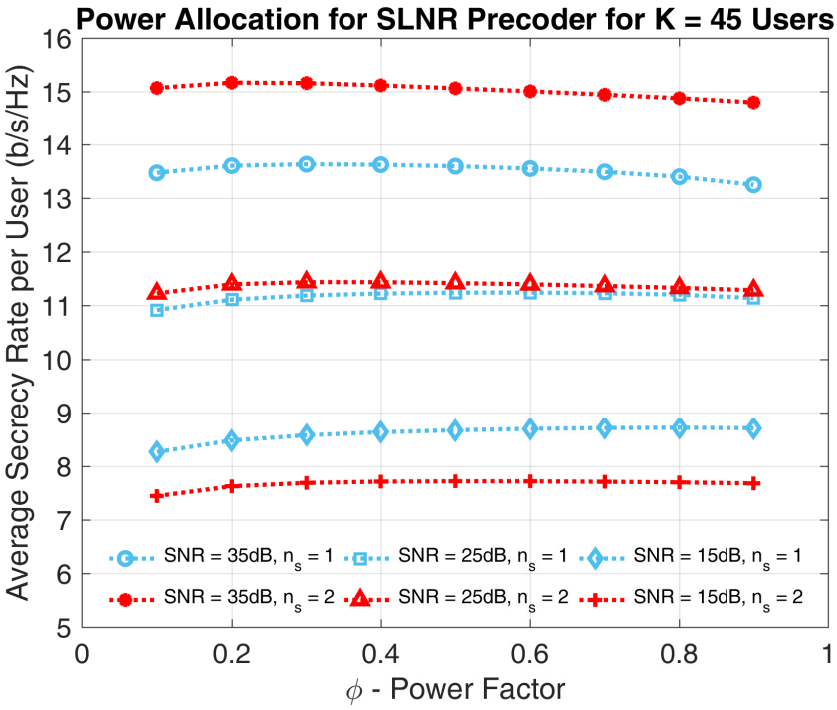

Figure 4.3. Average secrecy rate per user vs ϕ for SLNR precoder K = 45.

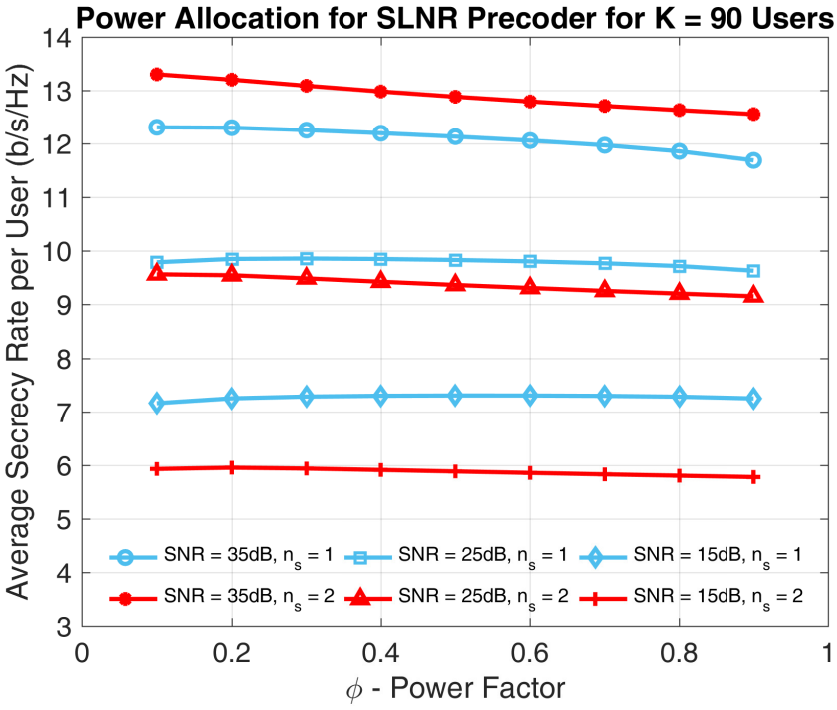

Figure 4.4. Average secrecy rate per user vs ϕ for SLNR precoder K = 90.

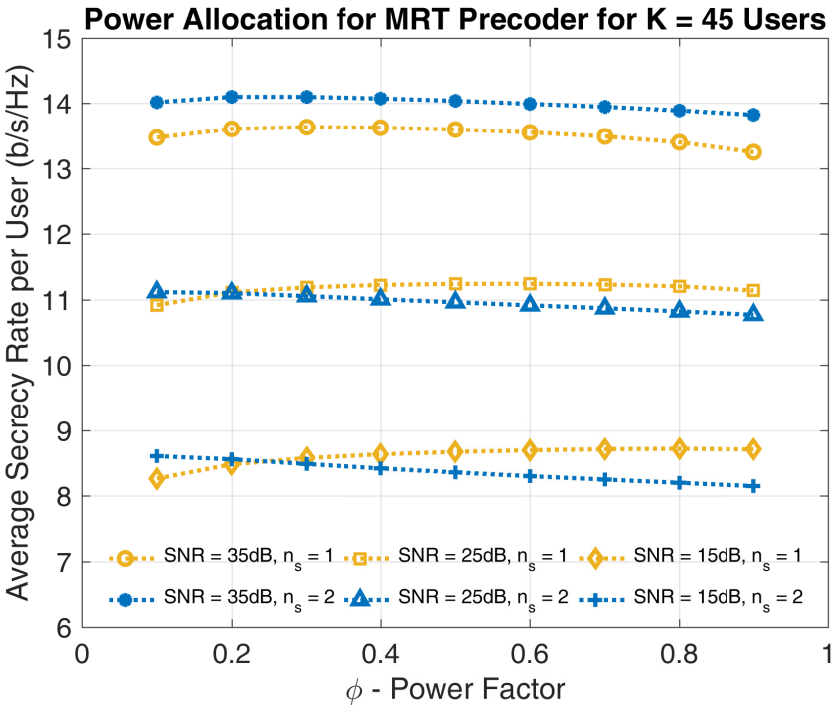

Figure 4.5. Average secrecy rate per user vs ϕ for MRT precoder K = 45.

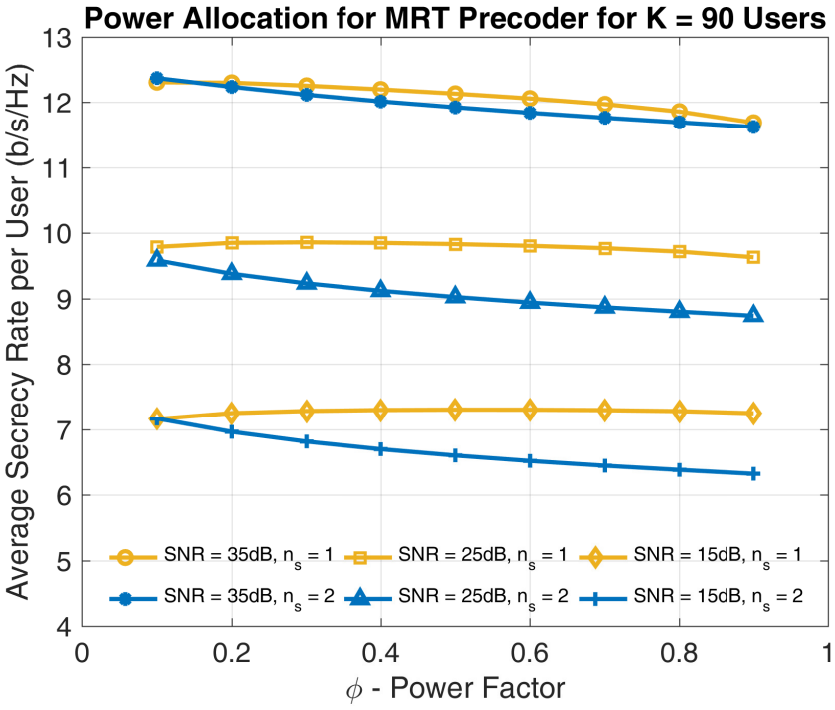

Figure 4.6. Average secrecy rate per user vs ϕ for MRT precoder K = 90.

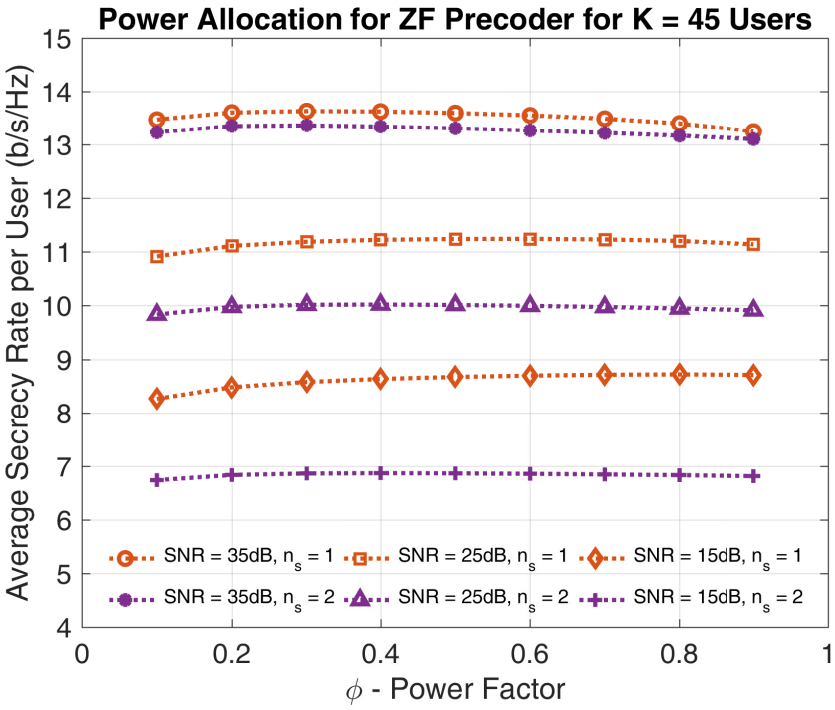

Figure 4.7. Average secrecy rate per user vs ϕ for ZF precoder K = 45.

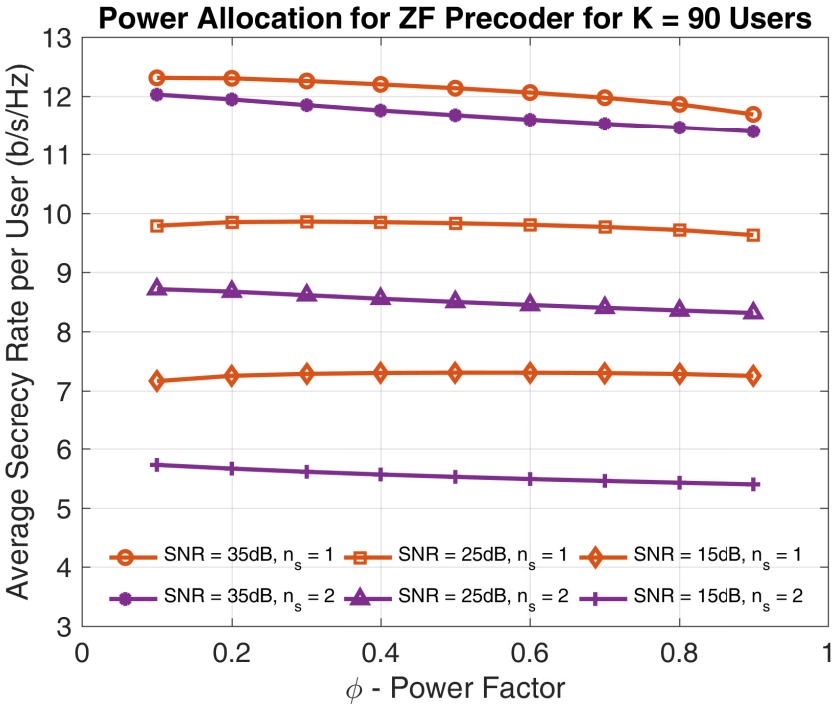

Figure 4.8. Average secrecy rate per user vs ϕ for ZF precoder K = 90.

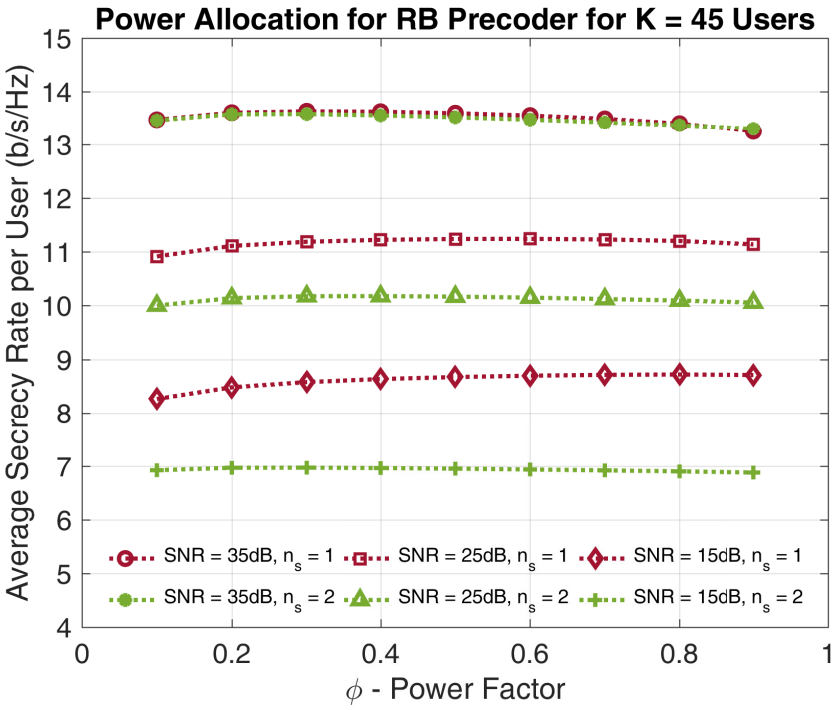

Figure 4.9. Average secrecy rate per user vs ϕ for RB precoder K = 45.

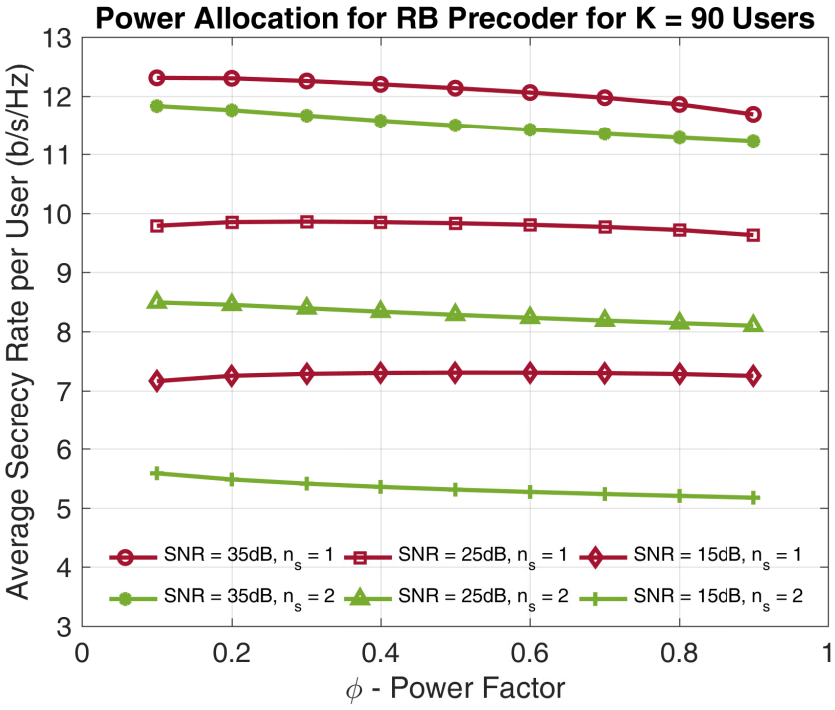

Figure 4.10. Average secrecy rate per user vs ϕ for RB precoder K = 90.

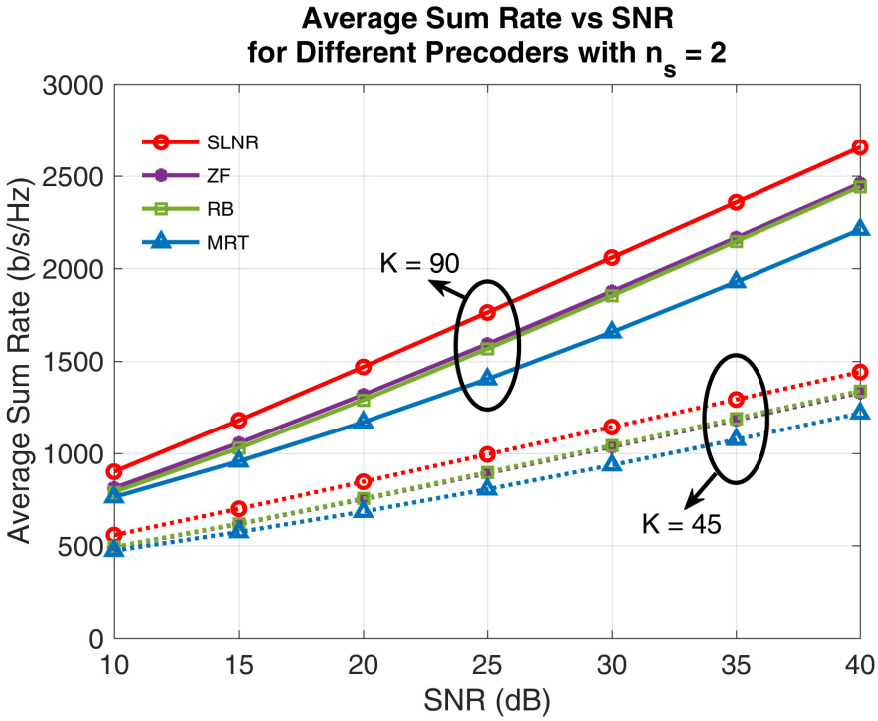

Figure 4.11. Average sum rate vs SNR for K and different precoders and $n_s = 2$.

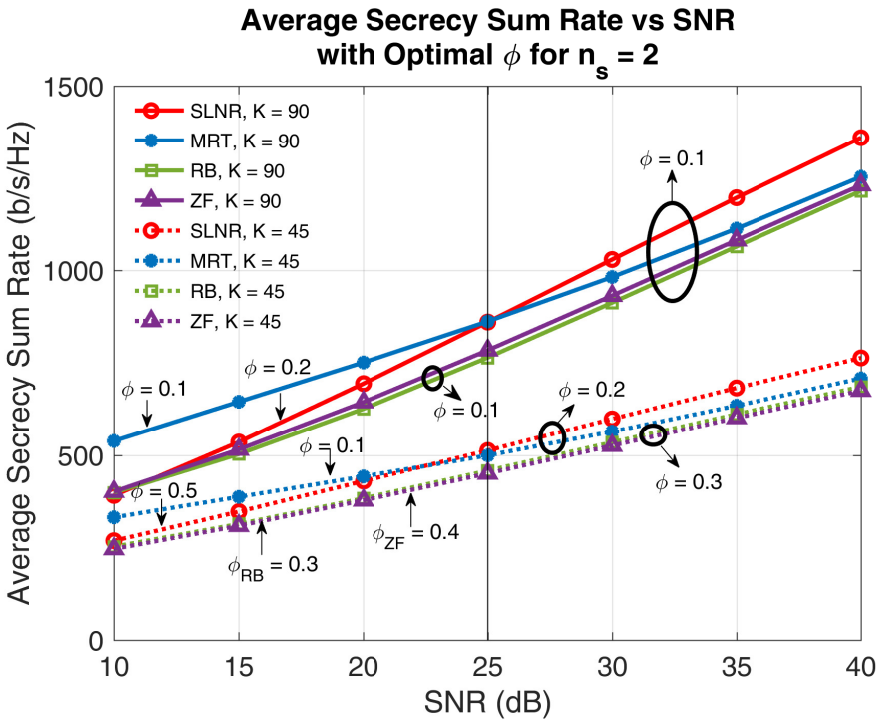

Figure 4.12. Average secrecy sum rate vs SNR for different precoders with optimum ϕ.

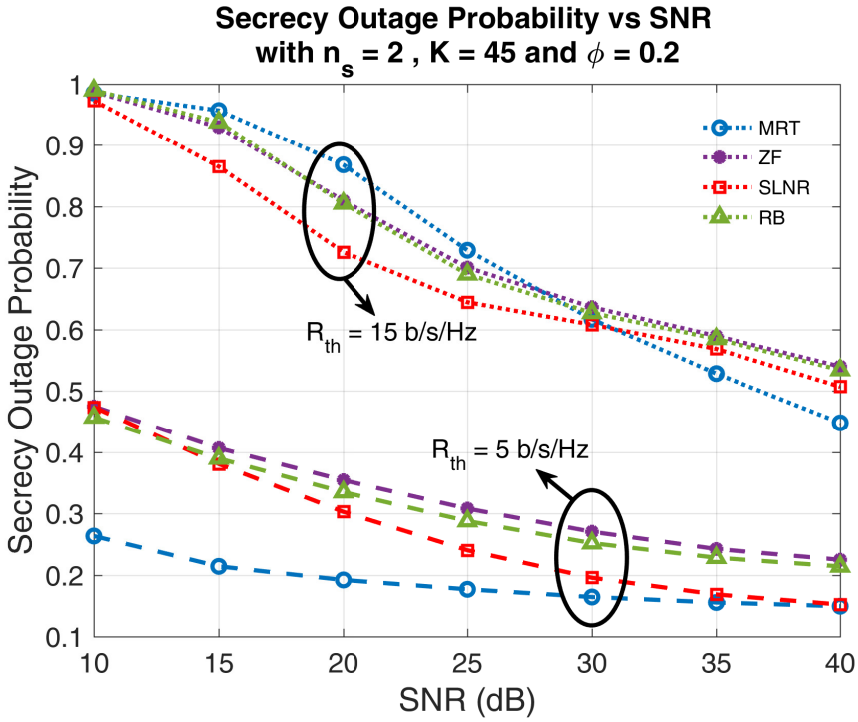

Figure 4.13. Secrecy outage probability vs SNR for K = 45 and $n_s = 2$ with $\phi = 0.2$.

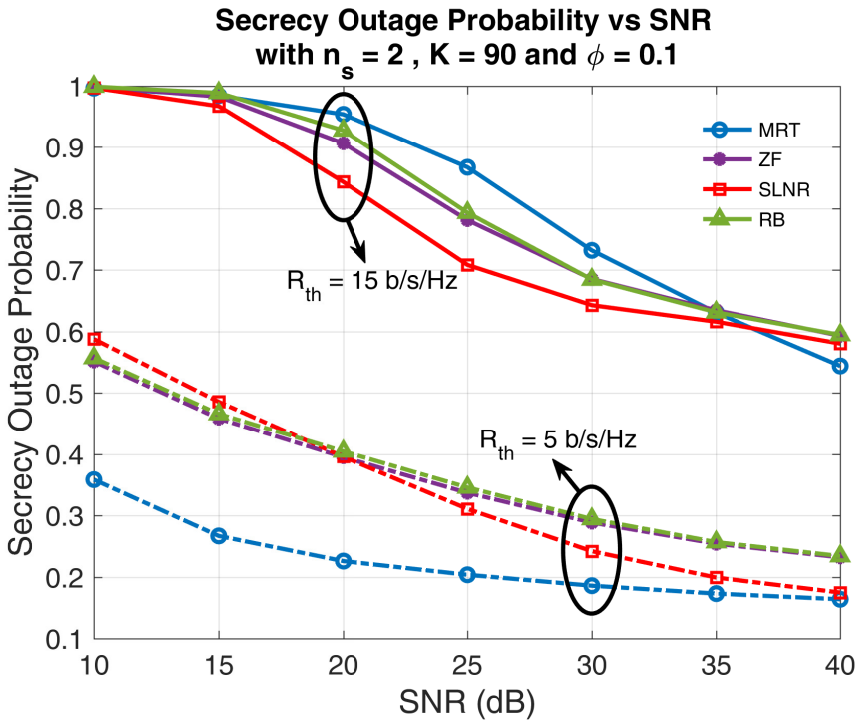

Figure 4.14. Secrecy outage probability vs SNR for K = 90 and $n_s = 2$ with $\phi = 0.1$.

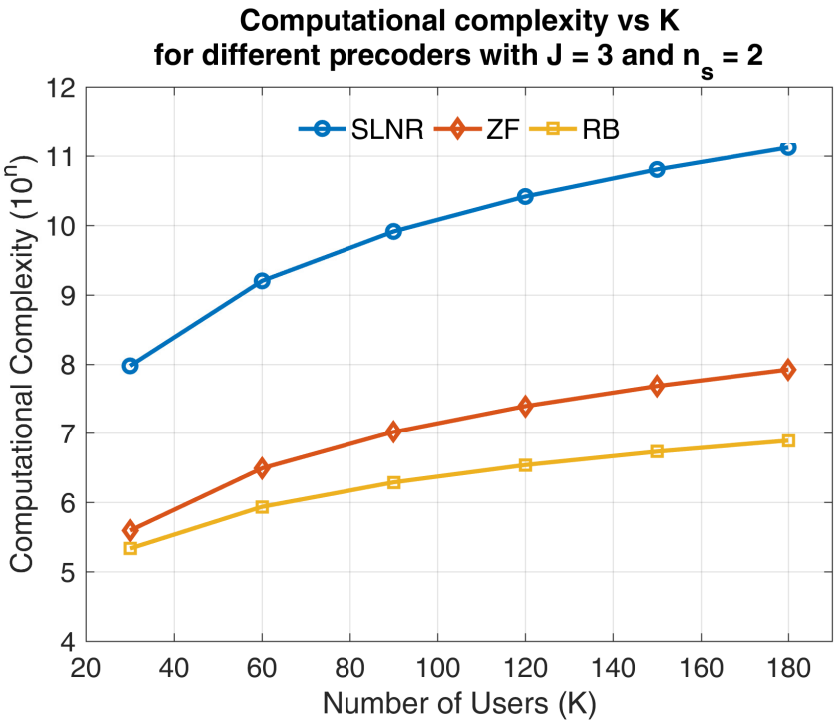

Figure 4.15. Complexity vs K for different precoders with J = 3 and $n_s = 2$.

CHAPTER 5

CONCLUSION

In this thesis, we have proposed different beamforming strategies for the physical layer security in the mmWave MU-MIMO networks. Since wireless networks are vulnerable to eavesdropping attacks due to their open natures, we have examined different practical scenarios for the mmWave MU-MIMO networks in terms of the average data rate, average secrecy rate and secrecy outage probability. Moreover, we have considered a hybrid scheme at both ends to provide a power-efficient system without compromising the number of antennas and the directivity.

Firstly, we have introduced the fundamental concepts such as mmWave channel modeling, massive MIMO systems and linear beamforming techniques, and hybrid scheme in Chapter 2 without considering the security yet. The mmWave channel is constructed using the statistical models. Since the mmWave channel includes LoS dominant and a sparse channel that has a limited number of resolvable paths, it has forced us to take into account the low-rank signal processing techniques. We have considered both the single stream and multiple streams in this thesis and the mmWave channel does not always have multiple paths, so two-streams are chosen for the multiuser scenarios. Also, we have given linear beamforming techniques for both single-user and multiuser cases in single-cell communication systems. The performance evaluations show that the system performance can be enhanced in terms of the average data rate when the number of antennas and the number of streams are increased. Furthermore, the large antenna arrays enable to use of simple linear beamforming techniques such as MRT with a significant improvement compared to its performance on the conventional communication systems. If the number of users in the systems increases, the linear beamforming techniques such as ZF and MMSE performs better for mitigating the interference that occurs among users and streams.

Secondly, we have examined the PLS in the presence of passive eavesdropper for a single-cell mmWave MU-MIMO communication in Chapter 3. We have proposed AN based beamforming method to make it compatible with the hybrid scheme. Generally,

AN precoder is obtained from the null-space of digital precoder for most of the cases. We have proposed to obtain AN precoder from the null-space of jointly designed digital and analog precoders of each legitimate user to reduce complexity. Nevertheless, we have used AN precoder to jam the channel of the eavesdropper and we have chosen MMSE precoder for mitigating interference among users and streams. For the performance results, we have first obtained the optimum power allocation factor between legitimate user precoder and AN precoder for the different number of users. Then, we have provided the average secrecy sum rate for the different number of users and streams with respect to their optimum power factors. We have discussed the effects of the number of users, the number of antennas at both BS and an eavesdropper, and the number of streams on the secrecy outage probability. The performance results show that the PLS can be enhanced by mmWave and MIMO beamforming techniques with using AN. It is also worth noting that the single stream provides more secrecy than multiple streams since the eavesdropper can get more information from nLoS instead of only LoS.

Thirdly, we have extended our scheme to the secure multicell mmWave MU-MIMO communication in Chapter 4. We have studied different linear beamforming techniques that are divided into coordinated and non-coordinated linear beamforming techniques. We have also employed two different beamforming techniques namely SLNR with CoMP and RB with non-CoMP that are the first exploration so far for the secure mmWave systems according to the best of our knowledge. The signal expressions, mathematical descriptions of PLS metrics, and hybrid scheme with AN precoder are also extended to the multicell scenario. By evaluating the performance results, we have first explored the optimum power allocation factor for different beamforming technique and each number of users. Then, we have compared them for both the average secrecy sum rate and the secrecy outage probability. Considering the multiple streams, while SLNR gives the best secrecy sum-rate performance since it utilizes the coordination among BSs, MRT gives interestingly the best secrecy outage minimization performance when both the threshold rates and the average SNR are low. On the other hand, the ZF and RB precoding give almost the same performance for both the secrecy sum rate and the secrecy outage probability. Since MRT requires less computation, it is useful for such systems when the number of antennas at the BSs is increased. However, if the number of users increases, it can be more wisely to choose ZF, MMSE, or RB instead of MRT to provide security and

to mitigate the interference. Although the coordination among BSs plays a huge impact on the performance of the system, the computational complexity is getting high when both the number of users and streams increases. Thus, SLNR should be considered twice since it is expected that the mmWave systems must satisfy the low latency applications with ultra-high reliability. However, RB can be considered as a good alternative for these systems and it can be further improved with novel algorithms. As a result, the PLS can still be improved by the mmWave and appropriate precoders with AN for the multicell mmWave communication systems.

Overall, we have presented a comprehensive study for the linear beamforming techniques considering the hybrid scheme in the mmWave MU-MIMO sytems. A general framework has been presented for the secure systems. The results show that the overall system performance highly depends on the power allocation factor between the signal of legitimate users and AN precoder, the SNR region, and the number of streams.

As future work, the PLS analysis can be extended to the different network topology such as NOMA, distributed MIMO, and cell-free cases in mmWave communications.

REFERENCES

Ahmed, Irfan and Khammari, Hedi and Shahid, Adnan and Musa, Ahmed and Kim, Kwang Soon and De Poorter, Eli and Moerman, Ingrid (2018). A survey on hybrid beamforming techniques in 5g: Architecture and system model perspectives. *IEEE Communications Surveys & Tutorials 20*(4), 3060–3097.

Alkhateeb, Ahmed and Mo, Jianhua and Gonzalez-Prelcic, Nuria and Heath, Robert W (2014). Mimo precoding and combining solutions for millimeter-wave systems. *IEEE Communications Magazine 52*(12), 122–131.

Chung, Jaehak and Hwang, Chan-Soo and Kim, Kiho and Kim, Young Kyun (2003). A random beamforming technique in mimo systems exploiting multiuser diversity. *IEEE Journal on selected areas in communications 21*(5), 848–855.

Csiszár, Imre and Korner, Janos (1978). Broadcast channels with confidential messages. *IEEE transactions on information theory 24*(3), 339–348.

El Ayach, Omar and Rajagopal, Sridhar and Abu-Surra, Shadi and Pi, Zhouyue and Heath, Robert W (2014). Spatially sparse precoding in millimeter wave mimo systems. *IEEE transactions on wireless communications 13*(3), 1499–1513.

Erdoğan, Oğulcan and Özbek, Berna (2020). Hybrid beamforming for secure multicell multiuser mmwave mimo communications. In *Physical Communication*. Elsevier (In preparation).

Erdoğan, Oğulcan and Özbek, Berna and Busari, Sherif Adeshina and Gonzalez, Jonathan (2020). Hybrid beamforming for secure multiuser mmwave mimo communications. In *2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*. IEEE (Accepted).

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

Golub, Gene H and Van Loan, Charles F (2012). *Matrix computations*, Volume 3. JHU press.

Hemadeh, Ibrahim A and Satyanarayana, Katla and El-Hajjar, Mohammed and Hanzo, Lajos (2017). Millimeter-wave communications: Physical channel models, design considerations, antenna constructions, and link-budget. *IEEE Communications Surveys & Tutorials 20*(2), 870–913.

Hong, Y-W Peter and Lan, Pang-Chang and Kuo, C-C Jay (2013). Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches. *IEEE Signal Processing Magazine 30*(5), 29–40.

Ju, Ying and Wang, Hui-Ming and Zheng, Tong-Xing and Yin, Qinye (2017). Secure transmissions in millimeter wave systems. *IEEE Transactions on Communications 65*(5), 2114–2127.

Khisti, Ashish and Wornell, Gregory W (2010a). Secure transmission with multiple antennas part i: The misome wiretap channel. *IEEE Transactions on Information Theory 56*(7), 3088–3104.

Khisti, Ashish and Wornell, Gregory W (2010b). Secure transmission with multiple antennas part ii: The mimome wiretap channel. *IEEE Transactions on Information Theory 56*(11), 5515–5532.

Lee, Gilwon and Sung, Youngchul and Kountouris, Marios (2016). On the performance of random beamforming in sparse millimeter wave channels. *IEEE Journal of Selected Topics in Signal Processing 10*(3), 560–575.

Lin, Jingran and Li, Qiang and Yang, Jintai and Shao, Huaizong and Wang, Wen-Qin (2017). Physical-layer security for proximal legitimate user and eavesdropper: A frequency diverse array beamforming approach. *IEEE Transactions on Information Forensics and Security 13*(3), 671–684.

Molisch, Andreas F and Ratnam, Vishnu V and Han, Shengqian and Li, Zheda and

Nguyen, Sinh Le Hong and Li, Linsheng and Haneda, Katsuyuki (2017). Hybrid beamforming for massive mimo: A survey. *IEEE Communications Magazine 55*(9), 134–141.

Mukherjee, Amitav and Fakoorian, S Ali A and Huang, Jing and Swindlehurst, A Lee (2014). Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Communications Surveys & Tutorials 16*(3), 1550–1573.

Ng, Derrick Wing Kwan and Lo, Ernest S and Schober, Robert (2014). Robust beamforming for secure communication in systems with wireless information and power transfer. *IEEE Transactions on Wireless Communications 13*(8), 4599–4615.

Ramadan, Yahia R and Minn, Hlaing and Ibrahim, Ahmed S (2017). Hybrid analog-digital precoding design for secrecy mmwave miso-ofdm systems. *IEEE Transactions on Communications 65*(11), 5009–5026.

Rappaport, Theodore S and Sun, Shu and Mayzus, Rimma and Zhao, Hang and Azar, Yaniv and Wang, Kevin and Wong, George N and Schulz, Jocelyn K and Samimi, Mathew and Gutierrez, Felix (2013). Millimeter wave mobile communications for 5g cellular: It will work! *IEEE access 1*, 335–349.

Sadeghzadeh, Mehdi and Maleki, Mehdi and Salehi, Masoud and Bahrami, Hamid Reza (2018). Large-scale analysis of physical-layer security in multi-user wireless networks. *IEEE Transactions on Communications 66*(12), 6450–6462.

Sadek, Mirette and Tarighat, Alireza and Sayed, Ali H (2007). A leakage-based precoding scheme for downlink multi-user mimo channels. *IEEE transactions on Wireless Communications 6*(5), 1711–1721.

Samimi, Mathew K and Rappaport, Theodore S (2016). 3-d millimeter-wave statistical channel model for 5g wireless system design. *IEEE Transactions on Microwave Theory and Techniques 64*(7), 2207–2225.

Shannon, Claude E (1949). Communication theory of secrecy systems. *Bell system tech-*

nical journal 28(4), 656–715.

Shen, Zukang and Chen, Runhua and Andrews, Jeffrey G and Heath, Robert W and Evans, Brian L (2006). Low complexity user selection algorithms for multiuser mimo systems with block diagonalization. *IEEE Transactions on Signal Processing 54*(9), 3658–3663.

Sun, Shu and Rappaport, Theodore S and Shaft, Mansoor (2018). Hybrid beamforming for 5g millimeter-wave multi-cell networks. In *IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 589–596. IEEE.

Swindlehurst, A Lee and Ayanoglu, Ender and Heydari, Payam and Capolino, Filippo (2014). Millimeter-wave massive mimo: The next wireless revolution? *IEEE Communications Magazine 52*(9), 56–62.

Tian, Xiaowen and Li, Ming and Wang, Zihuan and Liu, Qian (2017). Hybrid precoder and combiner design for secure transmission in mmwave mimo systems. In *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pp. 1–6. IEEE.

Vicario, Jose Lopez and Bosisio, Roberto and Anton-Haro, Carles and Spagnolini, Umberto (2008). Beam selection strategies for orthogonal random beamforming in sparse networks. *IEEE Transactions on Wireless Communications 7*(9), 3385–3396.

Wang, Dong and Bai, Bo and Zhao, Wenbo and Han, Zhu (2018). A survey of optimization approaches for wireless physical layer security. *IEEE Communications Surveys & Tutorials 21*(2), 1878–1911.

Wang, Shaoyu and Xu, Xiaoming and Huang, Kaizhi and Ji, Xinsheng and Chen, Yajun and Jin, Liang (2019). Artificial noise aided hybrid analog-digital beamforming for secure transmission in mimo millimeter wave relay systems. *IEEE Access 7*, 28597–28606.

Wu, Yongpeng and Khisti, Ashish and Xiao, Chengshan and Caire, Giuseppe and Wong,

Kai-Kit and Gao, Xiqi (2018). A survey of physical layer security techniques for 5g wireless networks and challenges ahead. *IEEE Journal on Selected Areas in Communications 36*(4), 679–695.

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

Xu, Jindan and Xu, Wei and Ng, Derrick Wing Kwan and Swindlehurst, A Lee (2019). Secure communication for spatially sparse millimeter-wave massive mimo channels via hybrid precoding. *IEEE Transactions on Communications*.

Yang, Nan and Wang, Lifeng and Geraci, Giovanni and Elkashlan, Maged and Yuan, Jinhong and Di Renzo, Marco (2015). Safeguarding 5g wireless communication networks using physical layer security. *IEEE Communications Magazine 53*(4), 20–27.

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