October 2019

Enhancing Secrecy and Capacity of Wireless Systems Using Directive Communications

Mohammed A. Hafez
University of South Florida

Enhancing Secrecy and Capacity of Wireless Systems Using Directive Communications

by

Mohammed A. Hafez

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
Department of Electrical Engineering
College of Engineering
University of South Florida

Major Professor: Hüseyin Arslan, Ph.D.
Nasir Ghani, Ph.D.
Ismail Uysal, Ph.D.
Jay Ligatti, Ph.D.
Tamer Khattab, Ph.D.

Date of Approval:
October 31, 2019

Keywords: 5G, Beam-Space, Directional Modulation, Multiple-Input-Multiple-Output (MIMO), Non-Orthogonal-Multiple-Access (NOMA), Physical-Layer-Security

Dedication

To my Parents and Sisters, for everything.

Acknowledgments

A desired respect and thanks for my parents who supported me since the beginning, and provided everything they can to raise me in the best possible environment. Also, a shout out to my two sisters who believed in me and supported me as much as they can.

Thanks to every teacher/professor spent from his/her time to teach me something new. Also, to my sports coaches for having the patience to help me develop new skills.

Thanks to my colleagues for providing support through the course of this trip.

Thanks to the coaches and crew mates of USF Rowing Club, for welcoming me into their friendly competitive family.

Special thanks to Dr. Tamer Khattab for providing a lot of support.

Special Thanks to Dr. Hüseyin Arslan for providing me the opportunity and the means to achieve this level, and having the patience to allow me to develop my skills.

Table of Contents

List of Tables

List of Figures

Abstract

The emerging advances in wireless communications make it an essential component of our everyday life. Moreover, the current research aims towards involving wireless communications in health monitoring applications, which helps medical personnel to remotely keep track of the development of the condition of their patients. Such information is considered highly sensitive and may cause significant harm if acquired by an adversary. The wireless environment has a broadcast type of nature, where the emitted electromagnetic waves spread all over the surrounding area of the transmitting antenna. This broadcast nature raises considerable concern about the secrecy of this sensitive information while being transmitted over-air.

On another side, the advancement in computer algorithms makes the currently adopted cryptographic algorithms prone to multiple attacks, which facilitate the access to the initially transferred information. In such a context, another approach is required to avoid the exposure of the information. Concealing the information at the physical layer of communications systems became of enormous interest to overcome the shortages in cryptographic approaches. One feature of the physical-layer is the availability of multiple transmit/receive antennas. The multiple antennas structure allows us to manipulate the spatial construction of the transmitted signals. The spatial construction of the signal allows us to limit the area, where any receiver in the system can detect the signal.

Our Studies focus on providing both secure and reliable communications, and we can characterize the studies in the following approaches,

- *Location-Based Secure Communications*: We established the ground for multiple directions transmission techniques, where each transmission direction carries an independent set of information. Using this ground, we proposed multiple approaches that limit the availability of the information to the small area surrounding the target receiver.

- *Complexity Reduction for Multi-Direction Systems*: With the increase in the physical resources, the complexity of the system increases. We proposed a simplified structure for the system that reduces the complexity from three orders of magnitude to a single order of magnitude. Moreover, we introduced a limited feedback scheme, that reduces the overhead used in the system.

- *Enhancing the System Capacity*: Due to the increase in the number of wireless users, higher data transmission rates need to exist. Using Directional transmission, we were able to intelligently allow the overlap of different data streams on the same available physical resource. This overlap allows the reuse of the same resource for different users, and increase the achievable transmission rates.

Chapter 1: Introduction

After the wireless communication advancement provided by different versions of long-term-evolution (LTE), the mobile wireless networks became a corner stone for most of our daily life activities. Moreover, with their widespread, the wireless paved the way for many new technologies, that were considered just as a futuristic vision a couple of years ago. 3GPP lunched the development of a new standard that will provide these emerging technologies with the required framework, namely 5G networks, also known as new-radio (NR) networks [1].

The NR framework is divided into three main categories. enhanced mobile broadband (eMBB), which is concerned with improving the services provided to the mobile end-user (e.g., increasing the throughput achieved by the user to get a better video streaming experience). ultra-reliable low-latency communications (URLLC), which is concerned by time sensitive applications (e.g., remotely operated machinery, and smart driving). massive machine type communications (mMTC), which is concerned by providing services for a high volume of devices (e.g., implantable medical devices). Each of these categories has a set of requirements that need to be met, an illustration of the 5G components and their relative requirements is represented in Table 1.1.

In order to fulfill those requirements, some key concepts were defined as enablers of the 5G networks. This includes, but not limited to:

Table 1.1: 5G-NR Service Categories and Requirements

Category	Requirements
Enhanced Mobile Broadband (eMBB)	• Very high capacity (10 Tbps/Km^2) • Very high data rates (100+ Mbps/user)
Ultra Reliable Low-Latency Communications (URLLC)	• High mobility support • Very low latency (1ms) • Very high reliability ($< 10^{-5}$ packet loss rate) • Strong security
Massive Machine-Type Communications (mMTC)	• High density (10^6 nodes/Km^2) • Low complexity • Low energy consumption • Cover challenging areas

- Flexible Waveform: As mentioned 5G is aimed to serve a wide variety of applications. Each of these applications has a different set of performance requirements, some would focus on total capacity, others will concern about latency. The current fixed frame structure, along with the strict waveform, will not be suitable to provide such experience. In order to cope with this variations, a flexible frame structure and waveform are needed. For the frame structure flexibility, the concept of numerology was introduced [2, 3]. while, for waveform, multiple variations were proposed (e.g., GFDM [4], FBMC [5], etc.).

- Massive MIMO: The huge number of antennas results in changing the structure of the wireless channel, and provides more degrees of freedom. Massive MIMO [6], reduce the processing load at the receiver side, which is beneficial for low power devices. Moreover, it has natural secure nature, which is necessary for the transfer of sensitive information. On the other side, it requires a full knowledge of the channel, which may not be practical.

- Millimeter Wave Communications: With the congestion of the currently used frequency bands (i.e., below 6 GHz), the move to the mm-Wave range opens a large space of possibilities [7]. The challenge in that range resides in the change of the wave propagation characteristics, where the signal attenuation is much larger. From another side, operating in mm-Wave range allows for a compact antenna arrays structures, which facilitate the deployment of several beam-forming approaches.

- Heterogeneous Networks: HetNets is a multi-tier network, with each tier serving a different set of users or applications [8]. The network can consist of a large coverage cell "*Macro Cell*", a small coverage cell "*Pico/Femto-Cell*", and a device to device tier "*D2D Link*". This tiered structure would highly facilitate the deployment of the multi-service system. The downsides of such structure include high overhead signaling and high latency.
- Non-Orthogonal Multiple Access: As the number of devices is expected to be enormous, and the available resources is always limited, either due to scarcity or technology limitations, sharing these resources between users is a necessity. NOMA [9] provides an approach to multiplex multiple users into the same resource, with an additional complexity to the users that can afford it. NOMA definitely increases the overall capacity of the system, but requires some intelligent and careful signal handling.
- Physical Layer Security: Because of the introduction of some IOT [10] applications to the wireless devices (e.g., remote operations, and medical monitoring [11]), more sensitive data transferred over the air. This huge amount of sensitive data need to be carefully handled in order not to fall in the hands of adversaries. Channel characteristics can be used to provide a secure communication link, with a trade off between the provided secrecy and limiting the capacity of the system, or increasing the complexity [12].

With These concepts in mind, the work presented here will be focusing on providing an enhanced multi-user experience in terms of both secrecy and total achievable rates. In order to provide such experience we will be using the directional ability of the multiple antenna systems. Directional transmission can be considered as a feature of both massive MIMO and mm-Wave communications. This is based on the fact that the large number of antennas and limited propagation conditions will make the communication channel more directional based. Besides, in order to stay in line with the 5G spirit, some algorithms will be proposed to reduce complexity and latency, which can make the suggested scheme have a more practical structure.

Directional transmission provide some sort of secrecy by default. This occurs because the signal is magnified towards a single direction while having a limited reach towards other directions. We will be utilizing this feature to further enhance the secrecy of all the users in the network. Moreover, This limited spread of the signal provide additional degrees of freedom that would allow achieving higher rates in a practical way. We will be taking advantage of this limitation to enhance the performance of the NOMA approach. This limitation helps reducing the amount of pre-processing required to multiplex the users under NOMA scheme.

The rest of this dissertation is organized as follows:

- in Chapter 2: we provide a review for the basic knowledge required in the area of multiple antennas systems and physical-layer security.
- in Chapter 3: we present some newly developed algorithms that targets the enhancement of secrecy and achievable communication rate.
- in Chapter 4: We discuss a practical training experience in the 5G-NR area.
- in Chapter 5: we conclude the presented work.

Chapter 2: Background

In this Chapter we will review some of the basic concepts, that the proposed solutions are build upon. First, we will review the multi-antenna systems, with different signal processing approaches and physical structures. Second, The channel models for these systems will be visited. Then, the concept of physical-layer security will be discussed. Finally, the basics of non-orthogonal multiple access (NOMA) will be reviewed.

2.1 Multi-Antenna System

The usage of multiple antennas for communications system caused a huge advantage in the mobile technology. The communication rate is limited because of the channel phenomenon called as fading. Fading is the fluctuations appear in the signal level due to delay-spread (frequency selectivity), Doppler-spread (time selectivity), and/or angular spread (spatial selectivity). With the limitations of transmission power and available frequency-bandwidth, fading is the limiting factor for possible increases in communication data rates. Introducing multiple antennas technology made it possible to increase the achievable rates, which would be linearly proportional to the number of used antennas. This section will discuss the benefits and drawbacks of multiple antenna system, along with transceiver design.

2.1.1 Benefits and Trade-Offs

Here we will present some of the benefits and trade-offs associated with the multiple antenna systems, and discuss the achievable limits for them.

- Array Gain: This refers to the increase in the received signal-to-noise-ratio (SNR) due to the coherent combining of the signals from different antennas. This combining can be realized at the receiver or transmitter side through maximal-ratio-combining (MRC)/maximal-ratio-transmission (MRT), respectively. This combining requires the knowledge of the channel-state-information (CSI) at the side performing the combining. This enhancement in SNR provides an increase in *coverage* of the network.

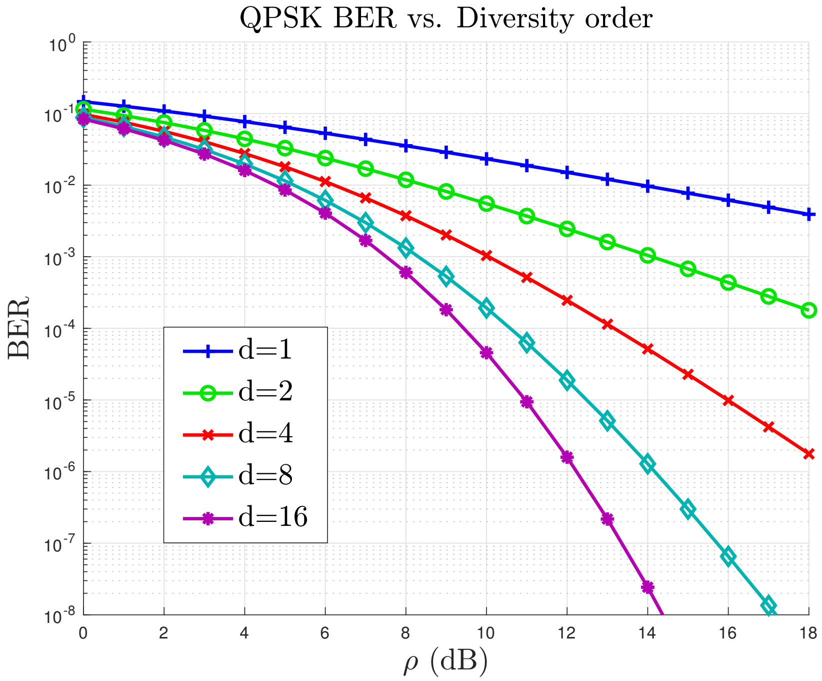


Figure 2.1: Diversity gain.

- Diversity Gain: Repetition is one of the effective coding methods that decreases reception errors. By sending multiple copies of the signal in different (almost independent) spatial dimensions, at least one of these copies will escape the deep fading situation. This degree of immunity to fading will provide better *reliability* for the received signal. The optimal diversity order will be $(d = N_T \times N_R)$, if all spatial channels are independent. Diversity gain can be given as,

$$d(R) = -\lim_{\rho\to\infty} \frac{\log_2 P_e(\rho,R)}{\log_2(\rho)}, \tag{2.1}$$

where ρ is the SNR and R is the rate. This translates as a change in the error rate slope, as shown in figure 2.1.

- Multiplexing Gain: Instead of transmitting the same data stream multiple times, multiple antennas offer the option of transmitting multiple independent data streams. The maximum number of independent data streams is limited by the communication channel condition, namely, the rank of the channel matrix. Ideally, with a full rank channel the number of independent stream is $(r = \min(N_T, N_R))$. Spatial multiplexing helps increasing the *capacity* of the network. The multiplexing gain is given as,

  $$r = \lim_{\rho \to \infty} \frac{C_{out}^{\gamma}}{\log_2(\rho)} \tag{2.2}$$

  where C_{out}^{γ} is the outage capacity when the outage probability is equal to γ. This reflects as an increase in the slope of the capacity. Although, diversity and multiplexing help decreasing error rate and increasing data rate, respectively, it is not possible to achieve both gains at the same time [13]. This trade-off is represented as,

  $$d(r) = (N_R - r)(N_T - r), \tag{2.3}$$

  which is illustrated in figure 2.2. This implies that for any increase in the transmission rate, an increase in the error rate is unavoidable.

- Interference Management: Interference in wireless networks results from multiple users sharing time and frequency resources. Interference may be mitigated in multiple-input-multiple-output (MIMO) systems by exploiting the spatial dimension to increase the separation between users. For instance, in the presence of interference, array gain increases the tolerance to noise as well as the interference power, hence improving the signal-to-

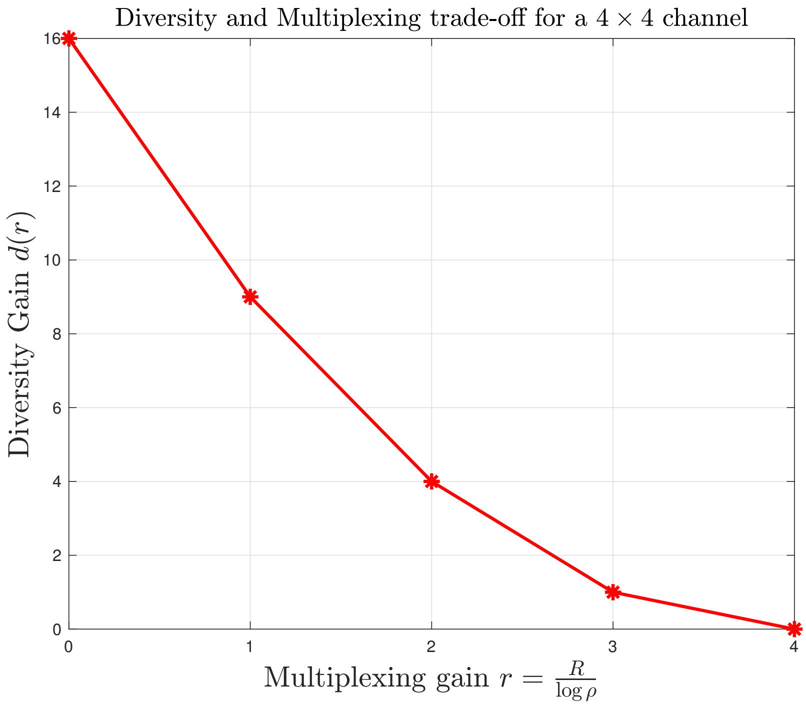


Figure 2.2: Diversity and multiplexing trade-off.

interference-plus-noise-ratio (SINR). Additionally, the spatial dimension may be leveraged for the purposes of interference avoidance, i.e., directing signal energy towards the intended user and minimizing interference to other users. Interference reduction and avoidance improve the coverage and range of a wireless network.

2.1.2 Transceiver Design

As mentioned in the previous section, there are different benefits of MIMO systems, which some of them can be utilized at the same time, and some cannot coexist. Based on the desired benefits, a different transceiver design is required. Here, we are discussing some basic algorithms of MIMO transceivers design.

- Space Time/Frequency Block Codes: Space Block coding are diversity schemes which can be applied either in time (e.g. Alamouti Scheme [14]), or in Frequency (e.g. LTE precoding). Taking Alamouti scheme as an example, with the assumption that the channel is invariant over two symbol periods, the transmitter sends two different symbols from different antennas in the first symbol period. Then in the second symbol period, it transmits a conjugate version of the same two symbols, as shown in figure 2.3. With the proper processing at the receiver side, Alamouti scheme can achieve a diversity gain of $2N_R$. Diversity schemes are beneficial for low rate/high reliability communications.

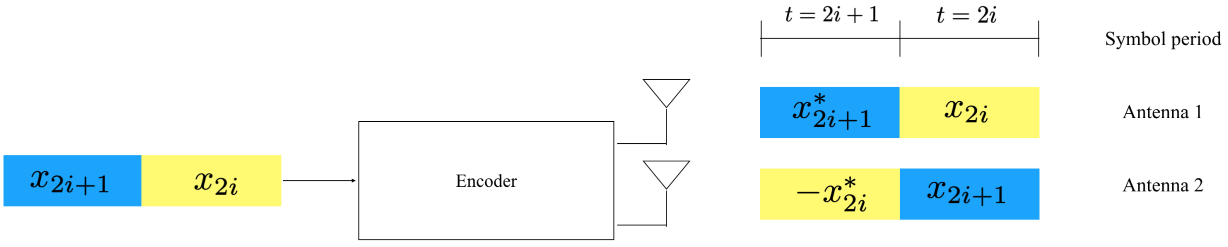


Figure 2.3: Alamouti scheme.

- Spatial Multiplexing: Differently, spatial multiplexing schemes is aimed to increase transmission data rates. The transmitter can transmit up to N_T different streams simultaneously, under the condition that $N_R \geq N_T$. In order to be able to separate the multiplexed streams, a special processing is required either at the transmitter or the receiver. The most famous multiplexing algorithms are zero-forcing (ZF) and generalized-singular-value-decomposition (GSVD), with both of them require the knowledge of the CSI at the processing side. Although, the maximum possible number of streams to be transmitted is $\min(N_T, N_R)$, a correlated spatial channel could limit that number to the rank of the channel. Spatial multiplexing scheme are desired for increasing the data rate while ignoring the communication reliability.

2.2 Spatial Channel Models

Communication channel modeling is an essential process that facilitate the system design process. Different channel models were proposed based on measurements and empirical fitting. The selection of the appropriate channel model is necessary, in order to be able to fairly judge the performance of an algorithm. Here, we discuss the different modeling perspectives regarding channel models for multiple antenna systems.

2.2.1 Statistical Models

Statistical channel model is the most widely used model. It treats the channel as a black box, the channel structure details are not important, only the distribution of the channel coefficients between each transmitting/receiving antenna pair is needed. This model has the advantage of simplicity, it can be easily implemented in a linear fashion [15]. The channel is represented as a matrix H of size $N_R \times N_T$, where N_R is the number of receiving antennas, and N_T is the number of transmitting antennas. Each element of the matrix $h_{i,j}$ represent the small scale fading coefficient between the i^{th} receiving antenna and the j^{th} transmitting antenna. With the received signal given as,

$$\mathbf{y} = \mathbf{Hx} + \mathbf{w}, \tag{2.4}$$

where $\mathbf{x} \in \mathbb{C}^{N_T \times 1}$ is a vector containing the samples to be transmitted from each antenna, $\mathbf{y} \in \mathbb{C}^{N_R \times 1}$ is the vector containing the received samples from the different antennas, and $\mathbf{w} \in \mathbb{C}^{N_R \times 1}$ is the noise added at each antenna with zero mean and variance σ_w^2. Figure 2.4 shows an illustration for the statistical model.

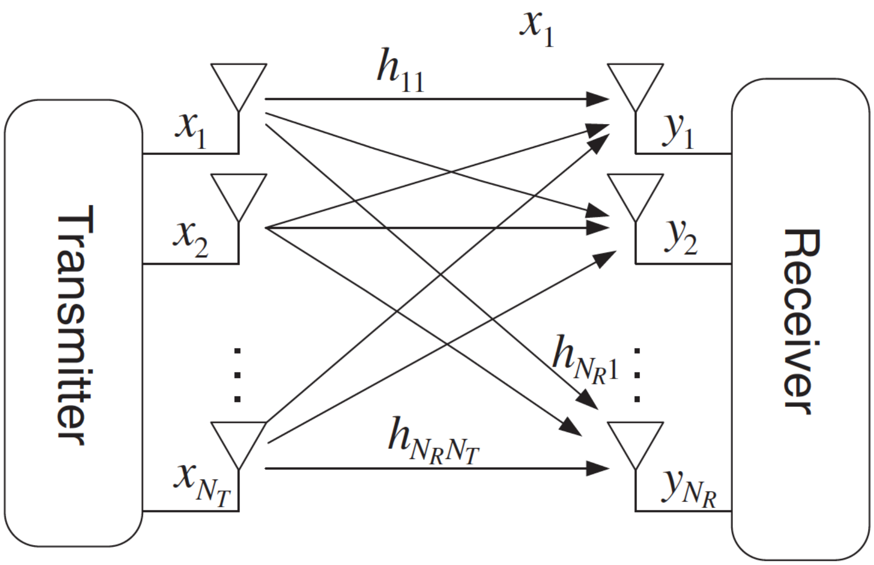


Figure 2.4: MIMO statistical channel model.

The channel capacity of the MIMO system depends on the knowledge available at the transmitter side about the communication channel. The capacity in general is given as,

$$C = \max_{f(x)} I(\mathbf{x};\mathbf{y}) \quad bits/channel\, use, \tag{2.5}$$

where $I(.)$ represents the mutual information. In case of CSI knowledge at the transmitter, the MIMO channel capacity is given by,

$$C = \sum_{r=1}^{R} \log_2 \left(1 + \frac{P\gamma_r \lambda_r}{N_T \sigma_w^2} \right), \tag{2.6}$$

where R is the rank of $\mathbf{H}$, P is the transmitted signal power, λ_r is the r^{th} unique Eigen value of $\mathbf{H}$, and γ_r is the power fraction allocated to the r^{th} Eigen vector. Given that $\sum_{r=1}^{R} \gamma_r = N_T$, The optimum solution for γ_r selection would follow the water-filing algorithm, as shown in figure 2.5, and the optimum value is given as,

$$\gamma_r^* = \left(\mu - \frac{N_T \sigma_w^2}{P\lambda_r} \right)^+, \tag{2.7}$$

In case of no CSI available at the transmitter side, the capacity is given as,

$$\begin{aligned} C &= \log_2 \left(\det \left(\mathbf{I}_{N_R} + \frac{P}{\sigma_w^2 N_T} \mathbf{H}\mathbf{H}^H \right) \right) \\ &= \sum_{r=1}^{R} \log_2 \left(1 + \frac{P\lambda_r}{\sigma_w^2 N_T} \right). \end{aligned} \tag{2.8}$$

The previously given expressions are for the deterministic channel case. In case of random channel, the Ergodic capacity averaged over different channel realizations can be used.

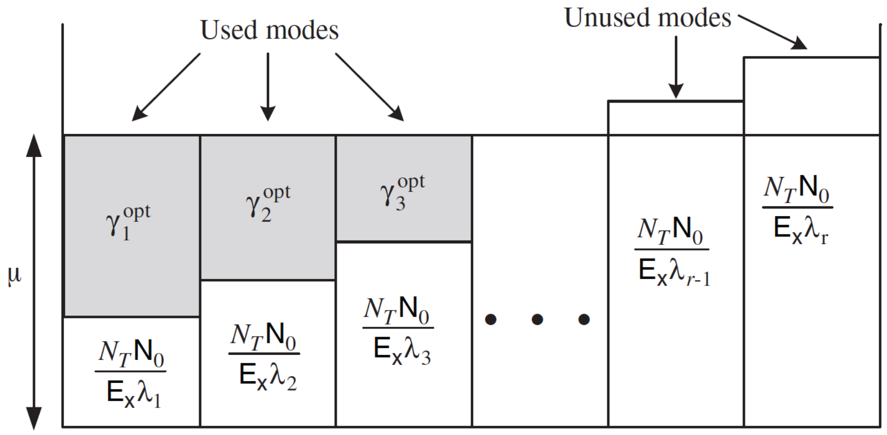

Used modes
Unused modes
μ
γ_1^{opt}
γ_2^{opt}
γ_3^{opt}
$\frac{N_T N_0}{E_x \lambda_1}$
$\frac{N_T N_0}{E_x \lambda_2}$
$\frac{N_T N_0}{E_x \lambda_3}$
$\frac{N_T N_0}{E_x \lambda_{r-1}}$
$\frac{N_T N_0}{E_x \lambda_r}$

Figure 2.5: Water-filing algorithm.

2.2.2 Physical Models

Contrary to the statistical model, the physical models are concerned about the actual structure of the channel [16]. The channel here is modeled in the angular domain instead of the spatial domain. The coefficients of the angular channel matrix can be given as,

$$h_{n,m}(t) = \sum_{l=1}^{L} \beta_l e^{j(2\pi f_l t+\zeta_l)} \mathbf{a}_R(\theta_n)\mathbf{a}_T^*(\phi_m)\delta(t-\tau_l), \tag{2.9}$$

where L is the number of paths. β_l, f_l, τ_l, and ζ_l are the gain, Doppler frequency, delay, and phase of the l^{th} path, respectively. $\mathbf{a}_R$ and $\mathbf{a}_T$ are the receive and transmit array steering vectors, respectively. The steering vectors depend on the geometrical structure of the antenna array. And the system can be represented as,

$$\mathbf{y} = \mathbf{A}_R \mathbf{H}_a \mathbf{A}_T^H \mathbf{x} + \mathbf{w}. \tag{2.10}$$

Although, the system is linear in terms of the channel coefficients, it is not linear in terms the transmit and receive angels θ_n and ϕ_m. An example for physical channel modeling is illustrated in figure 2.6, this follows the spatial channel model of 3GPP. As seen, the array steering vectors are a part of the model, which makes this model more suitable for analyzing the beam-forming based application.

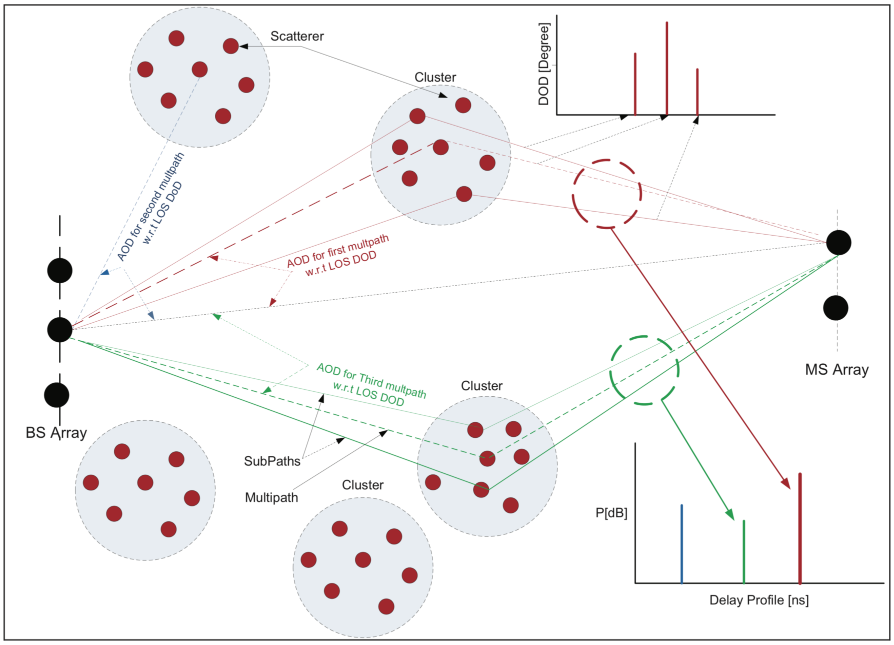

Scatterer
Cluster
DOD [Degree]
AOD for second multpath w.r.t LOS DoD
AOD for first multpath w.r.t LOS DOD
AOD for Third multpath w.r.t LOS DOD
Cluster
MS Array
BS Array
SubPaths
Multipath
Cluster
P[dB]
Delay Profile [ns]

Figure 2.6: Example of physical modeling “clustered delay line (CDL)”. [17]

2.2.3 Virtual Models

The virtual model takes a path in between the two other models. This model is currently highly adopted by the mmWave and massive MIMO research [18]. Instead of following the exact physical structure of the channel, The model considers that the channel consists of N virtual transmitting directions, and M virtual receiving directions, where N and M are the number of array elements at the transmitter and receiver, respectively. Hence, the channel matrix can be deconstructed as,

$$\mathbf{G} = \mathbf{A}_R \mathbf{G}_v \mathbf{A}_T^H, \tag{2.11}$$

where $\mathbf{A}_T = \left\{\alpha_{pq}^{(T)}\right\}_{N\times N}$ and $\mathbf{A}_R = \left\{\alpha_{pq}^{(R)}\right\}_{M\times M}$ are the steering responses of the array at transmitter and receiver, respectively. The matrix entries are given by,

$$\alpha_{pq}^{(T)} = \frac{1}{\sqrt{N}} \exp\left[-j2\pi\left(p - \frac{N-1}{2}\right)\frac{d}{\lambda}\cos\theta_q^{(T)}\right]. \tag{2.12}$$

where $p, q \in [0, 1, \ldots, N-1]$. The virtual directions here should represent orthogonal spatial basis, in order for them to reflect independent information about the channel. To insure orthogonality of these basis the directions $\theta_q^{(T)}$ should be selected as,

$$\theta_q^{(T)} = \arccos\left[\frac{\lambda}{dN}\left(q - \frac{N-1}{2}\right)\right], \tag{2.13}$$

and the same thing applies for $\mathbf{A}_R$, where $p, q \in [0, 1, \ldots, M-1]$. The selection of such basis will result in $\mathbf{A}_T$ and $\mathbf{A}_R$ exhibiting a DFT matrix structure.

$\mathbf{G}_v = \{g_{mn}\}_{M \times N}$ is the virtual channel matrix, which exposes some insights on the physical structure of the channel. For example, a dense matrix would reflect an environment rich in scatterers, while a sparse scattered matrix means that the channel has distributed sets of clustered scatterers. Figure 2.7 represents an illustration for the virtual channel model.

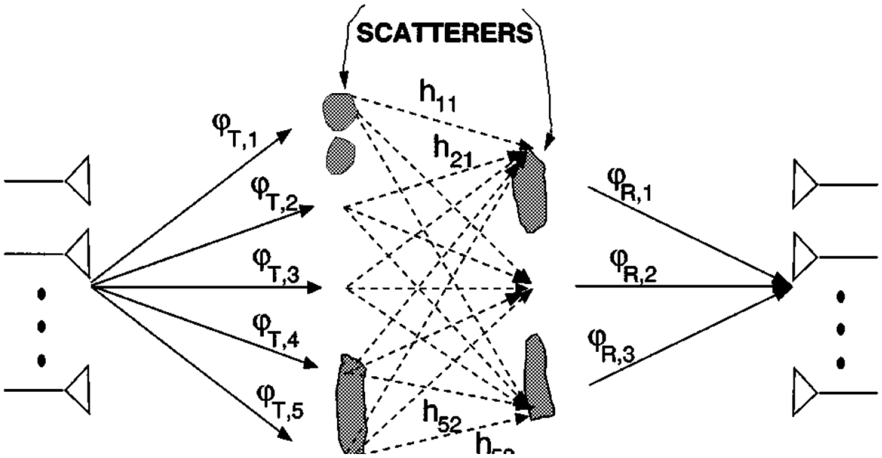


Figure 2.7: Virtual channel modeling.

2.3 Physical Layer Security

Due to the broadcast nature of the wireless communication channel, the transmitted signals over such channel are vulnerable to any malicious eavesdropping [19]. In order to secure the transferred information from such attacks, current standards depend on higher-layers cryptography algorithms, which are losing there effectiveness due to the increasing computational power of the current hardware. The retreat of higher-layer secrecy capabilities motivated the work on providing some security measures in the lower level (i.e. physical-layer).

For a secure communication link to be established, some kind of cooperation is required between the two legitimate terminals. That cooperation is aimed to put the eavesdropper in a disadvantage position. Shannon claimed that perfect secrecy can be achieved, if the transmitted code and the original message are mutually independent. The between the message and the code is done by using a key, which is shared excursively between the communication nodes. The existence of the possibility that the key may get exposed to the eavesdropper, makes the idea of perfect secrecy hard to implement.

Based on Shannon's information-theoretic point of view [20], Wyner developed the wire-tap channel model [21], which is considered as the basic structure for most of the physical-layer security problems. This work was extended to broadcast channels by Csiszar and Korner. In their work, they considered sending a common message to both receives, while equivocating a confidential message from one of them. Instead of sharing a certain key that can be exposed during the sharing process, the idea of using the common information about the communication channel was presented by Hassan. Integrating the channel knowledge into the ciphering process, revived the idea about perfect secrecy. Many proposals were made regarding the use of the channel, either by considering the channel information as the seed for the ciphering key [22], or by using the channel characteristics to conceal the message. The random nature of the physical-layer media promote it to be a good security tool, with the suitable use of signal processing algorithms. Besides, it doesn't require any additional processing in the upper layers.

Another aspect of secrecy is the authentication process. Before establishing a communication link, users need to verify the identity of the other node. Two types of attacks can fall under this category, namely, message falsification and impersonation. Again physical layer algorithm can be considered a mechanism to fight these attacks. The unique features, of each communication node in the network and the media between them, represents a good source of authentication process.

Multiple-Antennas (MA) systems offers more resources (i.e. degrees of freedom) to make use of the channel into secrecy. Some examples of these resources are the number of transmit antennas and the ability of having a directive communication by using antenna arrays. Using MA for secrecy purposes is a double-edged weapon, the enhanced transmission quality of the legitimate users is offset by the increased interception capabilities of the eavesdropper receiver. as with conventional MA techniques, the availability and accuracy of CSI plays a major role for regarding the system performance. One of the major techniques that compensate for imperfect CSI is the artificial noise transmission (i.e., the transmission of a jamming signal along with the legitimate signal). MA systems also allow the integration of multi-user techniques as means of secrecy [23,24] (e.g. broadcast MIMO wiretap networks, and MIMO wiretap channel with external cooperative helper).

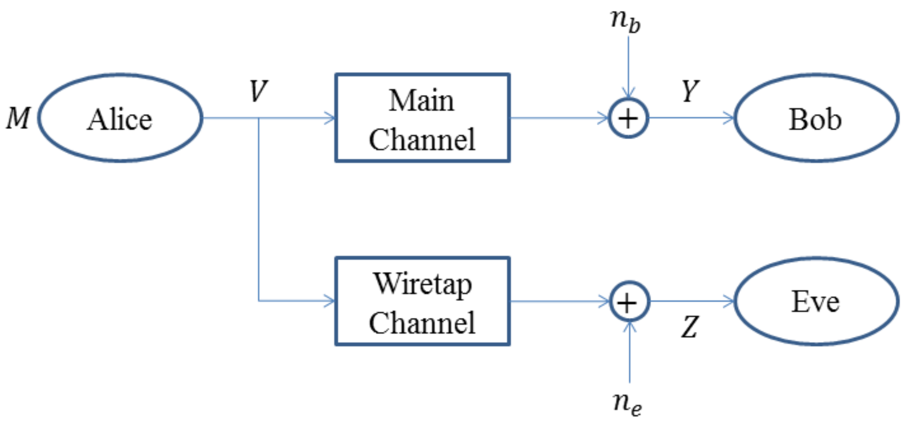


Figure 2.8: The wiretap channel model.

2.3.1 Wiretap Channel

The fundamental model of physical-layer security, called the *wiretap channel*, was introduced by Wyner [21]. This model represents the joint problem of reliable and secure communication over noisy channels. As shown in figure 2.8, the target of the transmitter (Alice) is to transmit a message M through the broadcast channel at a certain rate R. The message M should be correctly estimated $\hat{M}$ by the legitimate user (Bob), while the eavesdropper (Eve) should not obtain any information about M. Based on the aforementioned model, there exist a code that makes the secrecy communication rate R achievable, such that

$$\begin{aligned} \lim_{n \to \infty} \mathbb{P}(M \neq \hat{M}) = 0 \\ \lim_{n \to \infty} I(M; Z^n) = 0. \end{aligned} \tag{2.14}$$

The first condition here represent the reliable communication, while the second insures the secrecy. The assumptions associated with this model can be stated as,

- There is no existence for a shared key between Alice and Bob.
- The statistics of the channel and the code are known to all parties involved.
- the model assumes that authentication is already in place.

Based on these assumptions, the upper bound of all achievable rates, called *secrecy capacity*, is defined as

$$C_s = \max_{V \to X \to YZ} \left(I(V;Y) - I(V;Z) \right). \tag{2.15}$$

From (2.15), one can interpret that the secrecy capacity is the difference between the reliable communication rate $I(V;Y)$ and the information leaked to the eavesdropper $I(V;Z)$. This definition imply the following properties of the secrecy capacity,

- Secrecy capacity is positive, which require advantage between Alice and Bob (channel of eve is more noisy).

- Physical secrecy don't replace computational but help, as an example, we can use physical properties as means to refresh shared key instead of traditional key management.

Many approaches were proposed to design codes for physical-layer secrecy. two of the most popular approaches are "*channel capacity based codes*" and "*channel resolvability based codes*.

- Capacity based code:

  In this approach the designer choose code-words so that the corresponding uncertainty sets received by the eavesdropper do not overlap. Based on the wiretap channel model, we get $I(M;Z^n) = I(X^n;Z^n) - H(M^1) + H(M^1|MX^n)$. The information leaked about the message to Eve $I(M;Z^n)$ vanishes if two conditions are met: the randomness compensate the leaked information about the code-words $\frac{1}{n}H(M^1) \approx \frac{1}{n}I(X^n;Z^n)$, and the uncertainty is small $\frac{1}{n}H(M^1|MX^n) \approx 0$. This approach is easy to translate to a practical design, through LDPC and lattice codes.

- Channel resolvability:

  For that one, the designer tackle the variational distance secrecy (VDS) metric to induce a certain distribution for the received uncertainty sets at the eavesdropper. $\mathbb{V}(p_{MC^n}, p_M p_{C^n})$ is the VDS, which represents the distance between the joint distribution p_{MC^n}, of the message and the code, and the product of their marginal distributions ($p_M\ p_{C^n}$). Here, the overlapping between the uncertainty sets is allowed which turns the problem to a sphere covering problem, contrary to the sphere packing problem presented in the aforementioned approach.

2.3.2 Secrecy Performance Metrics

Here, we will introduce several of the most frequently used secrecy metrics. Some other metrics are applicable for certain case studies, but are not widely used.

- *Secrecy Rate*:

  The transmission rate that can be reliably supported on the main channel, but which is not decode-able on the interloper channel. the maximum achievable is the secrecy capacity. For multiple communication terminals case, one is interested in defining secrecy capacity regions [25].

  $$R_s = 0.5\log_2(\frac{1+\rho_b}{1+\rho_e}), \tag{2.16}$$

  where ρ_b and ρ_e are the received SNR by Bob and Eve, respectively.

- *Secrecy Outage Probability* (SOP):

  Represents the probability that a certain target secrecy rate γ_{C_s} is not achieved. SOP characterize the likelihood of simultaneously reliable and secure transmission [26]. employed in situations where only statistical CSI about the eavesdropper is available.

  $$P_{out}(C_s) = P(\tilde{C}_s < \gamma_{C_s}), \tag{2.17}$$

  where $\tilde{C}_s$ is the instantaneous secrecy capacity.

- *Secret Diversity/Multiplexing Gain*:

  Same as conventional MIMO, diversity is the asymptotic rate of decrease with SNR in probability of error at the desired receiver when subject to secrecy, while multiplexing (DoF) is the asymptotic rate of increase with SNR in the secrecy rate. the secret Diversity/ Multiplexing trade-off (DMT) capture the interplay between them [27]. DMT value highly depend on the amount of information available to the legitimate users about the main and wiretap channels.

- *Secret Key Rate*:

  It quantifies the rate at which legitimate users can agree upon a shared key sequence by exchanging messages over public channel [28]. This secret key rate $S(X;Y||Z)$ is lower and upper bounded by,

$$\begin{aligned} &S(X;Y||Z) \leq \min[I(X;Y), I(X;Y|Z)] \\ &S(X;Y||Z) \geq \max[I(X;Y) - I(Z;X), I(X;Y) - I(Z;Y)]. \end{aligned} \tag{2.18}$$

2.3.3 Multiple Antennas for PHY-Sec

MIMO systems are beneficial to use for many typologies and network layouts, and their use is extended to many applications. A summarizing of the usage of MIMO systems in the secrecy field is summarized by [29]. As our scope is limited compared to the extended of the MIMO usage in the secrecy field, we will be focusing on two main categories, namely, point-to-point MIMO and multi-user MIMO.

2.3.3.1 Point-to-Point

This topology includes a single transmitter (usually referred to as Alice), a single legitimate receiver (usually referred to as Bob), and an eavesdropper (referred to as Eve). Alice is trying to pass a confidential message to Bob, with minimizing the probability the Eve would be able to acquire it. This represent the very basic model that can be extended to various situations or topology.

- Design:

  Beam-former design mainly depends on the knowledge available at Alice about the channels of both Bob and Eve. Also, this knowledge determine the design target parameter, as mentioned in the secrecy metrics section. When perfect global knowledge about the channels is present at the transmitter, Alice can use ZF to eliminate the possibility of Eve receiving any information. The issue with ZF that it sacrifices some of the available degrees-of-freedom (DOF) in order to insure the secrecy of information. Also, This approach fails when Eve has a high number of receiving antennas [30].

Another beam-former uses GSVD to exploit the spatial dimensions where Bob has advantage over Eve. The GSVD creates a set of parallel single-input-single-output (SISO) channels, Alice then calculate the secrecy rate of each individual channel and transmits only at the channels where Bob has a positive secrecy rate. This approach achieves high secrecy performance, but it has a high computational complexity as well [31]. Other non-linear beamformers can be used to achieve better performance, but they involve a very high computational complexity.

The main problem with designing the beam-former for secrecy purposes is that the secrecy objective function (i.e., secrecy capacity/outage probability) usually cause the optimization problem to become non-convex. The non-convex complexity can be avoided by replacing the capacity objective function by some other convex functions, or some additional constraints can be added to generate a sub-optimal beam-former.

Another layer of secrecy, which can be added to some beamformers, is artificial-noise (AN) [32]. AN is placed to the null-space of the legitimate receiver channel, with a hope that it would degrade the channel quality of the eavesdropper. Because transmitters usually have a limited power budget, the available power is divided between the main channel and the AN. This raises a trade-off between the quality of the main channel, and the secrecy provided by the added AN.

- Power Allocation:

  Just considering increasing the total transmit power will not help enhancing the secrecy performance. This is because increasing the total power will enhance both the main channel and the wiretap channel. From this perspective, a careful power assignment to each spatial dimension is required [31]. Also, as mentioned before, in case on AN insertion the power allocation play a significant role on determining the performance. Moreover, with the rise of green communication concepts, energy efficiency became an important factor in systems design, which can also be achieved through efficient power allocation.

- Multiple Eavesdroppers:

  This situation is considered as a worst case scenario for secrecy systems. Multiple eavesdropper cases can be categorized in two approaches. First is the colluding eavesdroppers case, there eavesdroppers concurrently listen to the legitimate communication and cooperatively attempt to decode it. This also is similar to a single eavesdropper with spatially distributed antennas. In order for Alice to be able to provide secure communications, the available DOF should be larger than the number of eavesdropper. Due to the physical size limitation of the system, a secure communication could be inapplicable in such situation. also eavesdroppers are usually passive, which eliminate the possibility of placing the signal in the null space of the eavesdroppers, even with the addition of AN.

  Second is the non-colluding eavesdroppers. Here, the system performance is limited by the eavesdropper with the highest quality channel. Therefore, the design focuses on maximizing the minimum secrecy rate. This will ensure a secure communication link over all the other eavesdroppers.

2.3.3.2 Multiple Users

One of the multiple antenna system advances is supporting multiple users simultaneously, as mentioned before. Multiple users systems usually suffer from inter-user-interference. The interference can degrade the system performance, but also can be used to degrade the performance of the eavesdropper [33]. Here, we are discussing the design and performance of different multiple users channels.

- Broadcast:

  This represents the case of a single transmitter (base-station) sending different messages to multiple users in the down-link. Here two factors need to be considered in the secure system design, The amount of interference reflected on the legitimate receiver that degrades its performance, and the amount of data leakage that an eavesdropper would be able to collect. with appropriate pre-coding, AN is an appropriate way to degrade the eavesdropper channel quality while stay orthogonal to legitimate users [19]. Although, if CSI is imperfect at the transmitter, AN could cause degradation to legitimate users too. Another aspect to be considered for secrecy is users scheduling. Smart scheduling approach could help both reduce inter-user-interference, and increase secrecy performance.

  In Massive MIMO, due to the large number of antennas, high array gain, and fine spatial resolution, the expected information leakage can be neglected, even if the channel information of the eavesdropper is not available. This occurs due to the channel hardening feature of massive MIMO systems [34]. AN can be used with massive MIMO in order to add another layer of secrecy assurance.

- Multiple Access:

  Here, the multiple legitimate receivers are sending messages simultaneously to the legitimate receiver (base-station). In order to guarantee secrecy some sort of cooperation is required between the legitimate transmitters, this could be practically challenging due to the spatial separation of these transmitters. The area of multiple access secrecy is lightly explored, and only from the prospective of information theory. in [35], it was proved that the sum achievable secrecy DOF is $\frac{K(K-1)}{K(K-1)+1}$, where K is the number of users.

As mentioned before a good balance between secrecy performance and multi-user interference is necessary for multi-user multiple antenna systems. This balance requires a better knowledge of CSI and cooperation between users, which is practically challenging. Investigating distributed secure systems could help reduce these secrecy requirements, and it also can help in case of heterogeneous networks.

2.4 Non-Orthogonal Multiple Access

One of the technologies that support the aforementioned views and have drawn a huge attention lately is NOMA. NOMA is known for its superiority in terms of achievable capacity, flexibility, and adaptability towards a massive number of connections when compared to its counterpart orthogonal multiple access (OMA) [9, 36, 37]. These advancements will enhance the user experience for eMBB use case [38]. Moreover, the support of grant-free and asynchronous access is more applicable when NOMA is in use [39]. This will help to reduce the transmitted overhead and power consumption which will make the requirements for URLLC and mMTC achievable [40].

2.4.1 Power-Based

The majority of NOMA schemes are using power and code domains to multiplex users into the available resources. Other multiple access schemes like pattern division multiple access (PDMA) [41] and spatial division multiple access (SDMA) [42] are also related to NOMA. Power domain schemes main idea is exploiting the difference in the channel quality of each of the overlapped users [43]. While assigning a higher transmission power factor to the user with the weaker channel assure enhancing the received SINR at its end, the good condition of the channel of the other user allows it to deploy a successive interference cancellation (SIC) strategy that can help reducing the effect of the interference imposed on its signal [44]. Despite that power domain

NOMA is capable of supporting asynchronous transmission, it still requires a centralized control and scheduling. The advantage of NOMA over OMA can be seen in figure 2.9, it is clearly obvious that the capacity region provided by NOMA is much wider than OMA. This is only true under the condition of the existence of a decent SNR gap between the users sharing the spectrum.

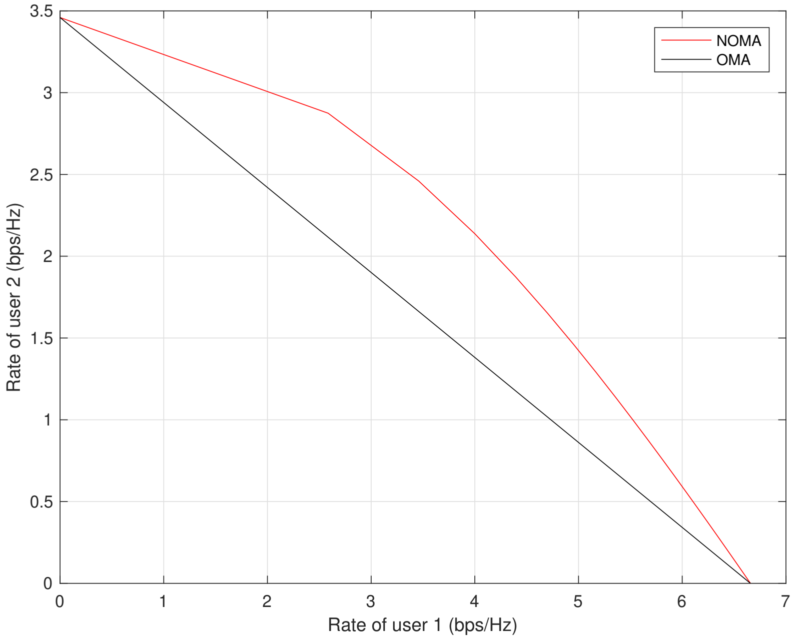


Figure 2.9: Capacity region for NOMA and OMA schemes

2.4.1.1 MIMO-OMA

MIMO systems divide the spatial domain into N orthogonal clusters. In order to avoid inter-cluster interference, the transmitter applies a precoding process based on the channels of the users assigned to each cluster. In order for the system to maintain the orthogonality while serving a number of users that is larger than N, the system divides time-frequency resources of each cluster between users sharing that cluster. If we assume that each cluster serves only 2 users, the sum achievable rate can be given as [45],

$$
\begin{aligned}
C_{\text{MIMO-OMA}} = \sum_{n=1}^{N} \Bigg[& \alpha_n \log_2 \left(1 + \frac{\rho_{2,n}|h_{2,n}|^2}{\alpha_n} \right) \\
& + (1-\alpha_n) \log_2 \left(1 + \frac{\rho_{1,n}|h_{1,n}|^2}{1-\alpha_n} \right) \Bigg].
\end{aligned} \tag{2.19}
$$

where $\rho_{i,n} = \frac{P_n}{\sigma_i^2}$ is the transmit SNR for the i^{th} user in the n^{th} cluster, P_n is the power assigned to the n^{th} cluster, and $\sigma_{i,n}^2$ is the noise power at the i^{th} user. $h_{i,n}$ represents the effective channel of the i^{th} user which include both precoding and fading effects, and α_n is the fraction of time-frequency resources allocated for the second user in the n^{th} cluster.

2.4.1.2 MIMO-NOMA

Similar to MIMO-OMA, the space is divided to N orthogonal clusters. Here, the system supports 2 users per cluster by allocating all the available time-frequency resource to both of them, while assigning a different transmit power for each of them based on their channel quality [46]. The system assumes the ability of one user to perform SIC, while the other user treating interference as additional noise. If we assume that the power fraction allocated to the second user in the n^{th} is Δ_n, then the sum achievable rate can be given as,

$$
\begin{aligned}
C_{\text{MIMO-NOMA}} = \sum_{n=1}^{N} \Bigg[& \log_2 \left(1 + (1-\Delta_n)\rho_{1,n}|h_{1,n}|^2 \right) \\
& + \log_2 \left(1 + \frac{\Delta_n \rho_{2,n}|h_{2,n}|^2}{(1-\Delta_n)\rho_{2,n}|h_{2,n}|^2 + 1} \right) \Bigg].
\end{aligned} \tag{2.20}
$$

Here, the first logarithmic term represents the achievable rate of the user applying SIC, while the second logarithmic term is the achievable rate of the user with the weak channel conditions. The denominator in the second term represents the interference effect from the other user, which is treated as noise. With such structure, some excess load is imposed on the scheduler for finding the suitable pair of users for each cluster. In order to combine two users under the same spatial dimension, their channels should be highly correlated. On the other hand, to be able to successfully employ SIC, the two users should have a decent SNR gap. This pairing process is done to minimize the interference leakage between clusters, and maximizing the overall gain.

2.4.2 Code-Based

On the other hand, Code domain NOMA spreads the data over the available resources to ensure high enough SINR for reliable data exchange. Code domain schemes can be categorized into two branches. The first branch is short sequence spreading, which uses short sparse codes with the deployment of an advanced symbol-level detector at the receiver such as message passing algorithm (MPA) (e.g. multi-user shared access (MUSA) [47], sparse code multiple access (SCMA) [48]). The second branch is long sequence spreading, which uses long codes to spread the data over all the resources with a deployment of a code-word-level SIC at the receiver (e.g. non-orthogonal coded access (NOCA) [49]). Both branches of code domain NOMA can support grant-free transmission. While the short sequences suffer from limited scalability due to the code length and the necessity of a synchronous transmission, Long sequences have a more complex receiver structure.

Chapter 3: Secrecy and Capacity Enhancing with Directional Transmission

In this chapter[1], we provide a detailed discussion about the new schemes we provided, in order to enhance the secrecy and capacity performance multiple antenna systems. These schemes are based on directional based communication. First, we will present the basic algorithm for Multi-beam transmission, which act as a baseline for all other techniques. Afterwards, we will focus on how to enhance the secrecy performance of the system, with different network topologies and channel conditions. Finally, we will show how to enhance the achievable rate of the system, by integrating the NOMA concept into directional communication.

3.1 Multiple Directions Transmission

When Directional modulation idea came into realization, the main focus of the research community was the algorithm efficiency, with the main focus was on a single direction transmission. Here, we proposed an extension to the directional modulation algorithm towards multiple directions transmission. With the ability to transmit multiple signals towards different directions simultaneously, extra degrees of freedom were provided, that can be used to achieve different goals, namely, reliability, secrecy, and quality.

3.1.1 System Characteristics

Consider a broadcast channel with a single source (base-station) and L destinations, namely directions. Each direction has its own desired data stream $x_i(k)$, and has a different transmission angle with respect to the base-station θ_i, where $i = 1, 2, \ldots, L$, and k is the time index. Different directions share the same resources of time slots, frequency bands, or codes simultaneously. The base-station uses a linear antenna array, with N elements, for transmission.

[1] Part of this chapter was published in [50–52]. Permission is included in Appendix A.

Based on the idea of directional modulation, we need to set $W = [w_1(k), w_2(k), \dots, w_N(k)]^T$, so that $f(\theta_i, k) = x_i(k)$, where W is the vector containing the complex weights for the antenna arrays, and f is the value of the resulting complex antenna pattern at a time instant k by the receiver located at a certain direction θ,

$$f(\theta, k) = h^*(\theta)W(k), \tag{3.1}$$

$$\begin{aligned} h^*(\theta) = [&e^{-j(\frac{N-1}{2})\frac{2\pi d}{\lambda}\cos\theta}, e^{-j(\frac{N-1}{2}-1)\frac{2\pi d}{\lambda}\cos\theta}, \\ &\dots, e^{j(\frac{N-1}{2})\frac{2\pi d}{\lambda}\cos\theta}] \end{aligned} \tag{3.2}$$

and $h^*(\theta)$ is the array steering vector for a receiver positioned at the direction θ.

Let us define F as the column vector that contains the desired pattern values, for each of the desired transmission directions.

$$\begin{aligned} F &= [f(\theta_1, k), f(\theta_2, k), \dots, f(\theta_L, k)]^T \\ &= H^H W = \begin{bmatrix} h^*(\theta_1) \\ h^*(\theta_2) \\ \vdots \\ h^*(\theta_L) \end{bmatrix} [w_1(k), w_2(k), \dots, w_N(k)]^T \end{aligned} \tag{3.3}$$

where, $H \in \mathbb{C}^{N \times L}$, and we consider that $L \leq N$, i.e., the number of desired transmission directions is less than the number of the antenna array elements. This makes (3.3) an under-determined linear equation. Using the least-norm solution [53], we will find that

$$W_{ln} = H\left(H^H H\right)^{-1} F \tag{3.4}$$

By replacing F with $X = [x_1(k), x_2(k), \dots, x_L(k)]^T$, we can produce the required weights to modulate the resulting antenna pattern, so that the pattern takes the desired values at the desired directions. Based on that, the value of the received pattern can be rewritten as,

$$f(\theta, k) = h^*(\theta)H(H^H H)^{-1}X(k) \tag{3.5}$$

Note that, the usage of any other antenna array structure is applicable, as long as the appropriate steering vector $h^*(\theta)$ is used for the generation of the weights W. Moreover, if we assume that the channel state information (CSI) for each of the users is available at the transmitter, we can enhance the secrecy performance of the system by multiplexing it within the generated weights.

$$W = A^H (AA^H)^{-1} X \tag{3.6}$$

where, $A = CH^H$, and C is the $(L \times L)$ diagonal matrix containing the CSI of each of the users.

For the sake of simplification, we take a look into the case, where we need to transmit in only two directions, we will find that the received signal at any arbitrary direction θ_s is

$$f(\theta_s, k) = \frac{1}{N^2 - y_{12}^2} \left[(N y_{s1} - y_{s2} y_{12}) x_1 + (N y_{s2} - y_{s1} y_{12}) x_2 \right] \tag{3.7}$$

where,

$$\begin{aligned} y_{pq} = y_{qp} &= \sum_{n=0}^{N-1} e^{j\left(n - \frac{N-1}{2}\right) \frac{2\pi d}{\lambda} (\cos\theta_p - \cos\theta_q)} \\ &= \frac{\sin\left(N \frac{\pi d}{\lambda} (\cos\theta_p - \cos\theta_q)\right)}{\sin\left(\frac{\pi d}{\lambda} (\cos\theta_p - \cos\theta_q)\right)} \end{aligned} \tag{3.8}$$

Based on (3.7), we can notice that, for the values of $\theta_s \approx (\theta_1, \theta_2)$, the received value of f is close to (x_1, x_2), respectively. Otherwise, the value of f oscillates around zero. Also, we can consider this as if we create some intended interference using the transmission of the other directions. The amount of this interference depends on the number of different directions L and the separation between these directions.

If we try to categorize the scheme based on the definition in [54], the used algorithm can be considered static for the case of single direction transmission. On the other hand, if we add one more transmission direction to the system, we will find that the scheme provides similar results as in the dynamic property. Fig. 3.1 shows the generated magnitude and phase of the transmitted pattern using QPSK signal structure.

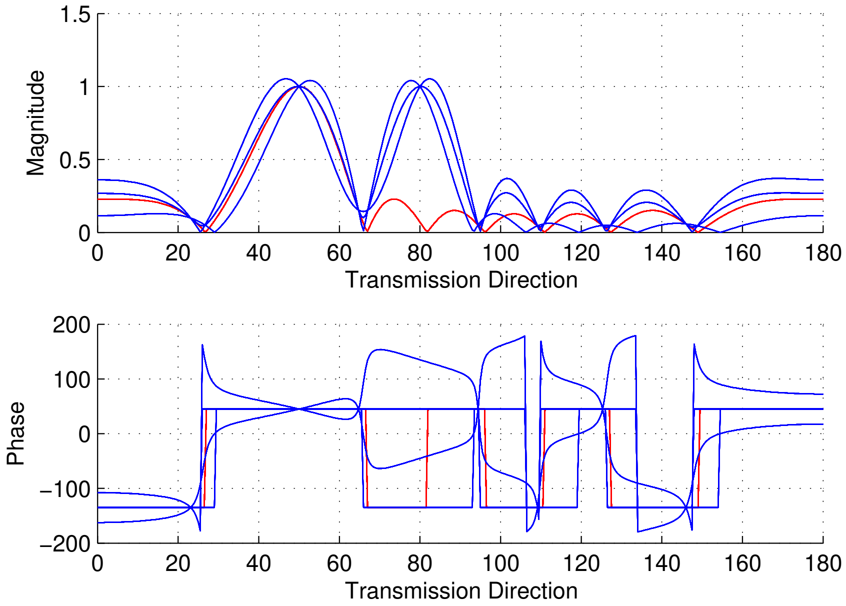


Figure 3.1: Transmitted pattern in case of two directions transmission. The upper section shows the magnitude of the received antenna pattern for each spatial direction, single intended direction transmission (red), two directions transmission (blue), users are located at 50^o and 80^o. The Lower section shows the phase of the received pattern with the same setup.

The system here transmits only the symbol $e^{j\frac{\pi}{4}}$ for the user located at 50^o, while transmitting a random symbol for the other user located at 80^o. We can see that in the case of single direction transmission (red curves), the magnitude and the phase of the resulting antenna pattern have a static value for all directions while, in the case of two directions (blue curves), the magnitude and the phase take multiple values depending on the transmitted symbol to the other direction. By increasing the number of directions to four (50^o, 80^o, 110^o, 140^o), we can recognize from Fig. 3.2 that the phase is becoming more random and may be considered as uniformly distributed on the values between $-\pi$ and π. Increasing the number of possible combinations of interfering symbols by using higher order modulation schemes, i.e., 16-QAM, 64-QAM, will definitely increase the randomization of the received signal outside the desired transmission beams.

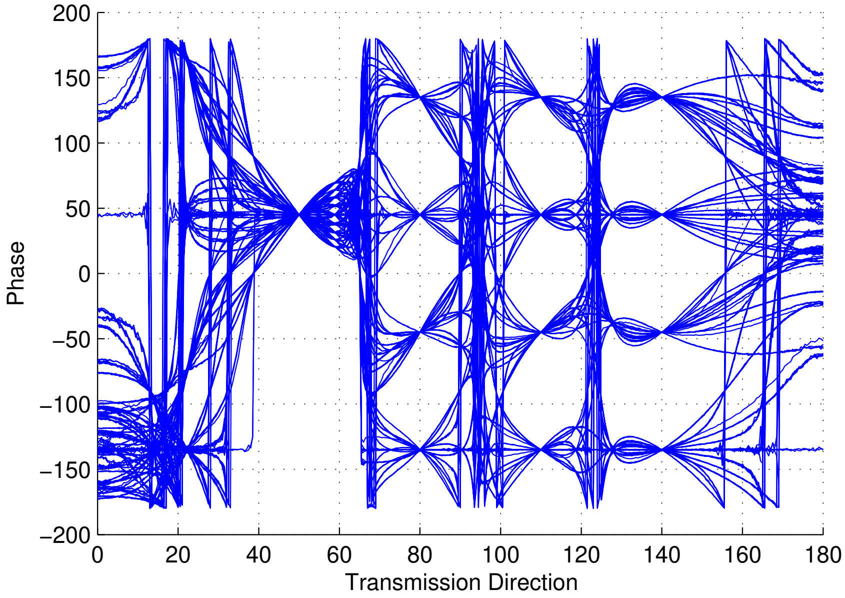


Figure 3.2: Phase Pattern in case of four directions transmission. The phase of the received antenna pattern at each spatial direction, the transmission is intended for 4 different directions, users are located at 50^o, 80^o, 110^o, and 140^o.

3.1.2 Reception Error Rate

Now, we will discuss the effect of this system structure on the error at the user-end. For BER evaluation, we use euclidean distance detectors for QAM, and a half-wavelength linear antenna array, with eight antenna elements (i.e. $N = 8$). The transmission is directed to 50^o, 80^o, 110^o, and 140^o, with an independent data stream for each of them. Fig. 3.3 and 3.4 show the error graphs for the reception obtained from 80^o direction, and the same apply for the other directions. We can rewrite (6) as

$$f(\theta_s) = [a_1(\theta_s), a_2(\theta_s), \ldots, a_L(\theta_s)] \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_L \end{bmatrix} \tag{3.9}$$

Based on that, we can define the signal-to-interference-plus noise- ratio (SINR) for the data stream i received at the direction θ_s as

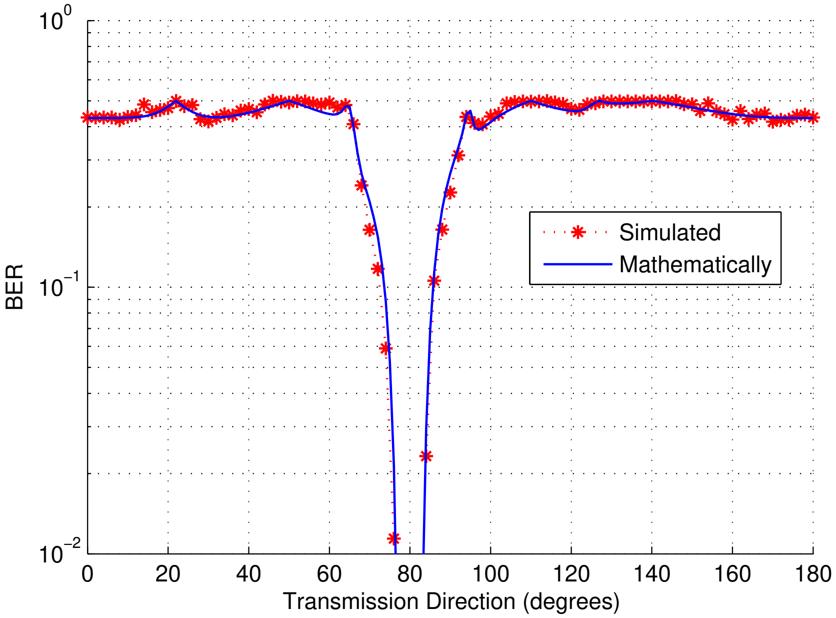


Figure 3.3: BER VS. transmission direction. Comparing the mathematical and simulated results of the BER of decoding the data directed towards 80^o. Here, we do not include the effect of the noise, so the figure shows only the effect of the interference created by the signals transmitted to other directions.

$$\rho_i(\theta_s) = \frac{|a_i(\theta_s)|^2}{\sum_{\forall j \neq i} |a_j(\theta_s)|^2 + N_{\theta_s}} \tag{3.10}$$

where $j \in \{1, 2, \ldots, L\}$.

Hence, the BER for a Gray-coded M-QAM modulation scheme (without channel coding) is approximated by:

$$BER_{QAM}(\theta_s) \approx \frac{\sqrt{M} - 1}{log_2(M) - 1} \left(\frac{log_2(M)}{\sqrt{M}} \right) Q \left(\sqrt{\frac{3\rho_i(\theta_s)}{M - 1}} \right) \tag{3.11}$$

where $Q(.)$ represents the Q-function, and M is the modulation order. In general, the lower bound of $BER(\theta_s)$ for any system can be calculated by substituting the value of the SINR by $\rho_i(\theta_s)$. This acts as a lower bound because it only considers the effect of the interference created by the signals of other users, and it does not include the distortion embedded to the signal by the DM algorithm.

In Fig. 3.3, we show the illustration of (11) in case of a 16-QAM transmitted signal. The result is compared to the one from the system simulation. Fig.3.4 shows the BER for different order QAM modulation schemes. It's obvious that when the modulation order increases, even though the effect of noise is neglected, the probability of error increases as we go far from the intended direction. This is noticeable through the change of the width of the main beam around 80^o.

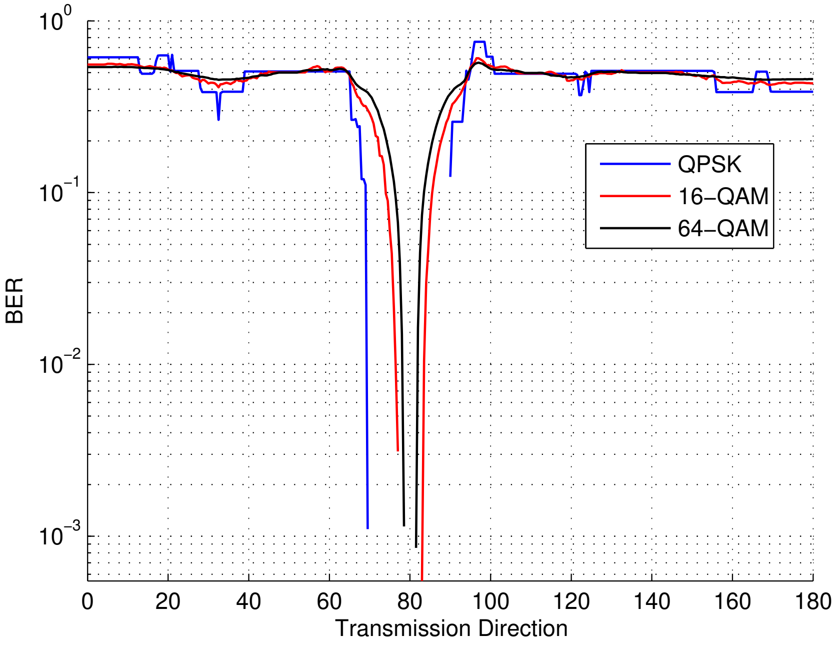


Figure 3.4: BER for different modulation orders. The BER of decoding the data directed towards 80^o, while using different modulation orders for the transmitted data.

In Fig. 3.5, we calculate the secrecy capacity based on effective SINR from (10), where the SNR for the desired direction at 80^o is 10 dB. Again, the figure shows high secrecy gain outside the main lobe, which indicates that the data obtained from non-intended directions will not be detected reliably. The figure also shows that the communication is not secure in the direction of the legitimate user, however, the multi-path nature of the channel can be used to generate a pre-coding scheme that insure secrecy for that direction. The precoder generation is out of the scope of this work.

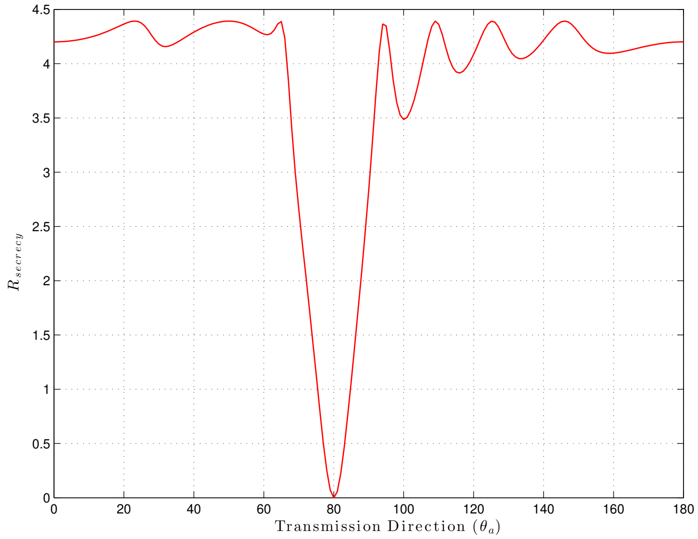


Figure 3.5: Secrecy rate vs. direction of transmission. the secrecy capacity calculated based on the SINR of the received symbols.

The secrecy capacity $C_{Secrecy}$, and capacities of the channels are obtained from

$$C_{Secrecy} = C(\theta_d) - C(\theta) \tag{3.12}$$

$$C(\theta) = log_2(1 + \rho_i(\theta)), \tag{3.13}$$

where $C(\theta_d)$ is the capacity at the desired direction θ_d.

What we noticed from the previous discussions is that, with the increasing number of the possible values of the transmitted signal, the randomness of the received signal outside of the interest beam increases. Also, the width of the correct reception beam decreases. Considering the extreme situation where the signal has the same structure as the noise, i.e., a Gaussian signal, orthogonal-frequency-division-multiplexing (OFDM) as an example, we can highly reduce the probability of detection outside of the main interest beam. Besides, the usage of an OFDM signal will facilitate the estimation and equalization of the effects of fading channels. For the OFDM system we used the Extended Pedestrian A (EPA) propagation model from the LTE standard [55], and the first OFDM symbol of each transmitted block is allocated for pilot signals to be used for channel estimation. It's assumed that the pilot signals are known for all the receivers in the system. Fig. 3.6 shows the BER for all the transmitted data streams with the direction of the transmission. We can see that each stream can be delivered correctly to a pre-specified direction, while it is observed as noise-like signal in other directions. The figure also shows the advantage of including the CSI as mentioned in (3.4). We can notice that having CSI as a part of the signal generation reduces the width of the detection beam (dashed curves). Here, CSI adds another source of randomization for the signal transmitted to the undesired directions.

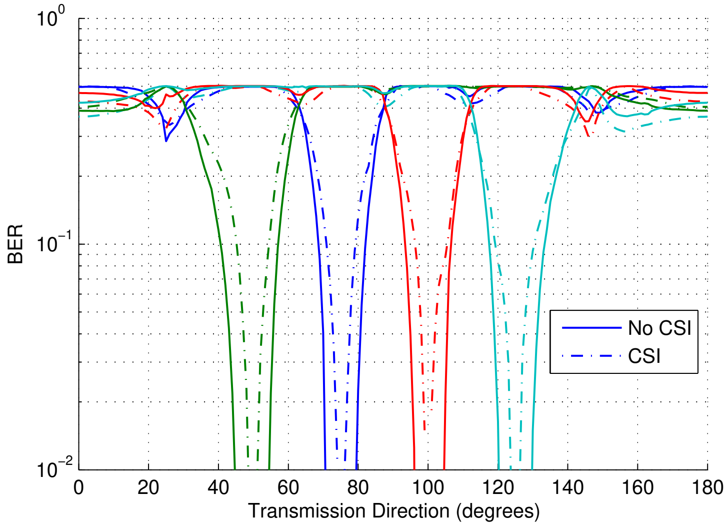


Figure 3.6: Channel knowledge effect on BER. Each of these curves represents the resultant BER at each direction, based on decoding each one of the transmitted streams. There are 4 different data streams directed to 50^{o}, 75^{o}, 100^{o}, and 125^{o}

As we expect to have large dimensions for H, and due to the high complexity of the matrix inversion operation, we suggest to employ least-mean-squares (LMS) adaptive filtering algorithm [56] to synthesize this system with low complexity. The algorithm is shown in Algorithm 1, and the value of the convergence factor μ is determined based on the construction of H. One of the main concerns about LMS is the convergence rate, which would affect the pattern generation rate, and the transmission rate. There are many other different techniques that can be used to generate the pattern, each of them has its own complexity and rate parameters (e.g., Recursive least squares (RLS), QR Decomposition, etc.) [56].

Algorithm 1 Complex LMS algorithm

```
$W(0) = \text{zeros}(N,1)$
while $c \geq 0$:
    $E = X^H - W(c)^H H$
    $W(c+1) = W(c) + \mu H E^H$
```

3.1.3 Flexible Beam-Width

As mentioned previously, the ULA response acts as an inverse DFT-process that performs a transformation from the spatial-location domain to the spatial-angular domain. Hereby, we suggest that it is possible to control the spatial-angular domain by integrating a DFT-process in the generation of the array weights. Figure 3.7 shows the block diagram for the proposed generation process of the array weights. This structure imitates an OFDM system structure but with both the DFT and its inverse located at the transmitter, with the sub-beams here resembling the sub-carriers in the OFDM case.

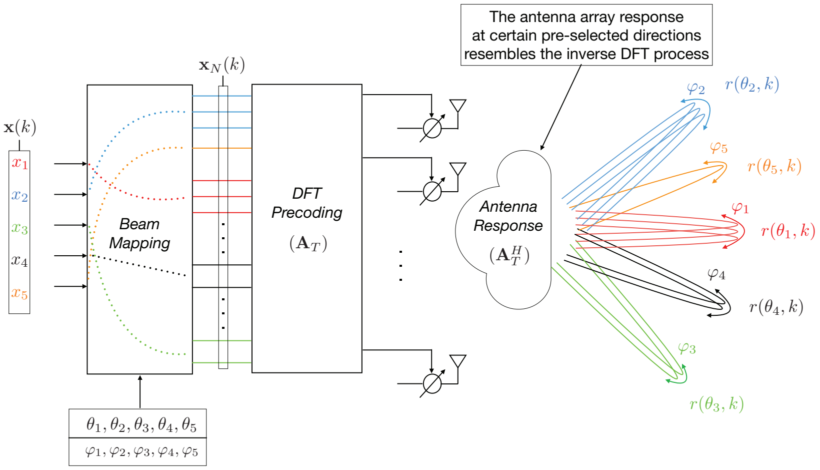


Figure 3.7: DFT-based directional modulation block diagram.

Then, the array weights can be generated using,

$$\mathbf{w}(k) = \mathbf{A}_T \mathbf{x}_N(k), \tag{3.14}$$

where $\mathbf{x}_N(k)$ is a $N \times 1$ vector containing the data to be transmitted $x_n(k)$ mapped to their corresponding sub-beams (angles) indexes. The system structure in (3.14) has several benefits,

- The generation matrix $\mathbf{A}_T$ is a fixed matrix, which makes it independent of the desired transmission directions θ_i. This independence will simplify the adaptation process in case of change in one of these transmission. Only the sub-beam assignment[2] will need to be changed.

- The generation matrix has a DFT structure, which makes the weights generation process less complex and more computationally efficient by implementing it using FFT-algorithm, compared to the previously suggested zero-forcing scheme.

- With the availability of large size arrays, this structure gives the flexibility in controlling the total beam-width assigned for each transmitted stream. If one stream requires a large beam-width[3] , assigning a set of sub-beams to the same stream would serve as a single large beam that satisfies the required width.

Moreover, directional modulation structure provides a secure communication path for each of the data streams. The signal delivered to any receiver will take the form,

$$r(k) = \mathbf{G}\mathbf{w}(k) + z(k) = \mathbf{A}_R \mathbf{G}_v \mathbf{x}_N(k) + z(k), \tag{3.15}$$

where z is a complex additive white Gaussian Noise.

[2] The sub-beams assignment is included in the vector $\mathbf{x}_N(k)$, where the vector $\mathbf{x}(k)$ is mapped to the desired directions, and the other elements of $\mathbf{x}_N(k)$ are equal to zero.

[3] This can occur if there is a larger area of coverage requirement or the receiver is suffering from a blockage

Based on the adopted model of single antenna receiver and single path channel, $\mathbf{A}_R = 1$, and $\mathbf{G}_v = \{g_n\}_{1\times N}$. If we consider a subset of the transmission directions, $\mathscr{N} \subset \{\theta_n\}$, composed of all the sub-beams affecting the intended receiver, then,

$$|g_n| = 0 \qquad \forall n \notin \mathscr{N}. \tag{3.16}$$

We define another subset of sub-beams, $\mathscr{P} \subset \{\theta_n = \theta_p\}$, composed of all directions (sub-beams) which contain the transmitted information $x_p(k)$, $p \in [1, 2, \ldots, P]$. Therefore,

$$r(k) = z(k) \qquad \forall n \notin (\mathscr{N} \cap \mathscr{P}). \tag{3.17}$$

Equation (3.17) refers to the case where the receiver is aligned to any of the virtual directions that are not utilized (i.e., x_n=0). In such case there is no information transmitted towards the location of that receiver. The secrecy concerns rise in two situations,

3.1.3.1 The Eavesdropper is Aligned to the Information Beam

In such case, several methods can be applied. One way would be exploiting the multi-path environment. The extension of the proposed scheme to multi-path channels can be straightforward similar to the suggestions in [51]. Also, a cooperative scenario can be beneficial [57].

3.1.3.2 The Eavesdropper is Out of the Information Beam

Contrary to (3.17), the eavesdropper receives a mixture of all transmitted streams. Here, we can make use of the similarity between the proposed scheme and OFDM structure by applying some OFDM based secrecy method (e.g. reducing the out-of-band transmission). Alternatively, the insertion of artificial noise into the non-utilized sub-beams (nulled virtual directions) would be effective, but it needs careful management in case of multi-path environment to avoid self-interference.

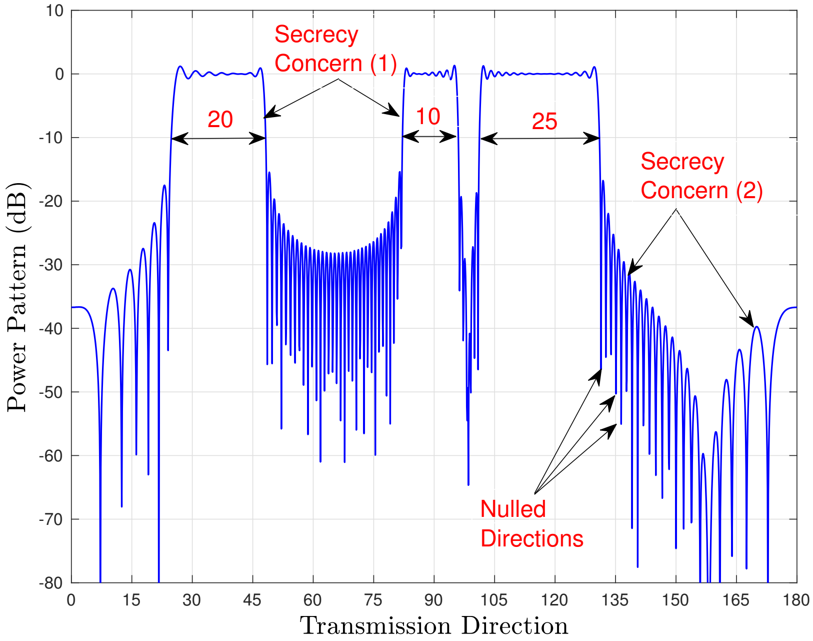


Figure 3.8: DFT-based transmission pattern. The transmitted power pattern with three different desired directions, and different beam-width requirements.

Such case can be represented by a mismatch between the generation matrix $\mathbf{A}_T$, and the transmission steering matrix $\tilde{\mathbf{A}}_T$, and the received signal will be,

$$r(k) = \mathbf{G}_v \tilde{\mathbf{A}}_T^H \mathbf{A}_T \mathbf{x}_N(k) + z(k). \tag{3.18}$$

This resembles the case of OFDM transmission with inter-carrier-interference due to sampling offset. Using [58, Eq. 22], we can define the average received power of the desired symbol at a certain direction, normalized to the symbol power, as

$$\eta(\theta) = \frac{\sin^2\{\pi\beta(\theta)N_s\}}{N_s^2 \sin^2\{\pi\beta(\theta)\}} \tag{3.19}$$

where $\beta(\theta) = \Delta\theta/\pi$, and $\Delta\theta = |\theta_d - \theta|$ is the difference between the direction of the desired symbol and the direction of the eavesdropper.

Hence the received SINR at the eavesdropper for the symbol x_p would be

$$\gamma(\theta) = \frac{\eta_p(\theta)}{\sum_{i \neq p} \eta_i(\theta) + \sigma_z^2}. \tag{3.20}$$

Figure 3.8 shows the transmitted power pattern. We can see the flexibility provided by the proposed scheme in terms of using variable sub-beam assignment to achieve beam-width change.

3.2 Location-Based Secrecy

A directional-based secrecy was discussed in the previous section, with different implementation strategies, considering flexibility and complexity. Although, the proposed scheme provides a secure communication link towards the desired direction, an eavesdropper located along the same direction would cause a huge secrecy threat. In this section, we will further enhance the proposed scheme, in order to avoid the man-in-the-middle issue.

3.2.1 Topologies

3.2.1.1 Single Transmitter

Consider a single base station equipped with an N elements linear antenna array. The base station is serving M legitimate users; each is equipped with a single antenna. We assume the existence of a passive eavesdropper, which is equipped with an arbitrary number of antennas N_E.

The signals transmitted by the M users are received through L different paths. Here, we assume space reciprocity, i.e., the signal transmitted by the base station is also received by the users through the same L paths. Note that; L is the maximum number of independent paths in the system [4].

[4] In a practical system, some of the users may experience less diverse channel. For these situations, the gain coefficients corresponding to the non-utilized paths by a user will be considered as zeros.

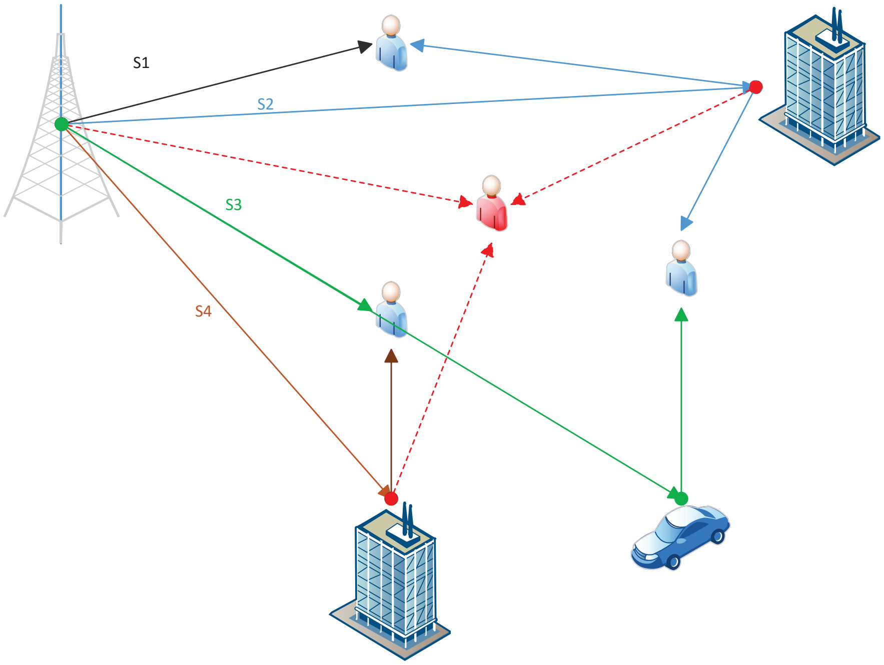


Figure 3.9: Single transmitter topology. A system illustration with 3 legitimate users (Blue) and one eavesdropper (Red). Legitimate users receive signals from 2 paths (Solid colored lines), and the eavesdropper receive it through 3 paths (Red dashed lines).

Let us define α_{ml} as the gain coefficient of the l^{th} path that is delivered to the m^{th} user. We assume that all α_{ml}'s are available at the base station through feedback from all users. Each path is delivered with θ_l angle-of-departure (AoD), these AoD's are evaluated at the base station, which can be done using one of the methods according to [59].

The eavesdropper receives signals through P paths, we also define β_p as the gain coefficient of the p^{th} path to eavesdropper. We assume that all β_p's and α_{ml}'s are also available at the eavesdropper. This is considered as worst-case scenario where the eavesdropper has acquired the information about the channel state information (CSI) of the legitimate link through feedback channels. Fig. 3.9 shows an example illustration for such system.

Here, we are considering random small scale fading effect, which is modeled as a Rayleigh fading. Then, the gains are modeled as i.i.d Gaussian random variables. The effect of the large scale fading (Path-loss and Shadowing) is not considered. This assumption is based on considering a noiseless channel for the eavesdropper. In such situation, for a certain eavesdropper location, the average path-loss affecting both the desired signal and interfering signals will almost have the same value, which means that the path-loss will not affect the value of the received signal-to-interference-ratio (SIR).

3.2.1.2 Coordinated Multi-Point Transmission

CoMP refers to a wide range of techniques that enable dynamic coordination or transmission with multiple geographically separated base stations to enhance the end-user service quality even at cell edges [60, 61]. One of the major categories for CoMP downlink transmission is the joint processing and transmission scheme where data is transmitted simultaneously from all base stations to improve the received signal quality or to cancel interference from other users. To that end, highly detailed feedback is required on the channel properties in a fast manner. Another requirement is the need for very close coordination between the base stations to facilitate combination of data as well as fast switching of the cells. Figure 3.10 shows the structure of CoMP network.

Here, we assume the lack of knowledge of CSI of all users at all base stations. Each base station only knows the relative direction of each desired user to its location. Moreover, the strict timing coordination can be relaxed since we are sending the same data from all base stations. Hence the delayed signals can be considered equivalent to multi-path components.

Considering a single user system, the received signal at the desired location will be,

$$r_d(t) = \sum_{i=1}^{B} g_i(t-\tau_i)s_{\text{Conf}}(t) + z(t), \tag{3.21}$$

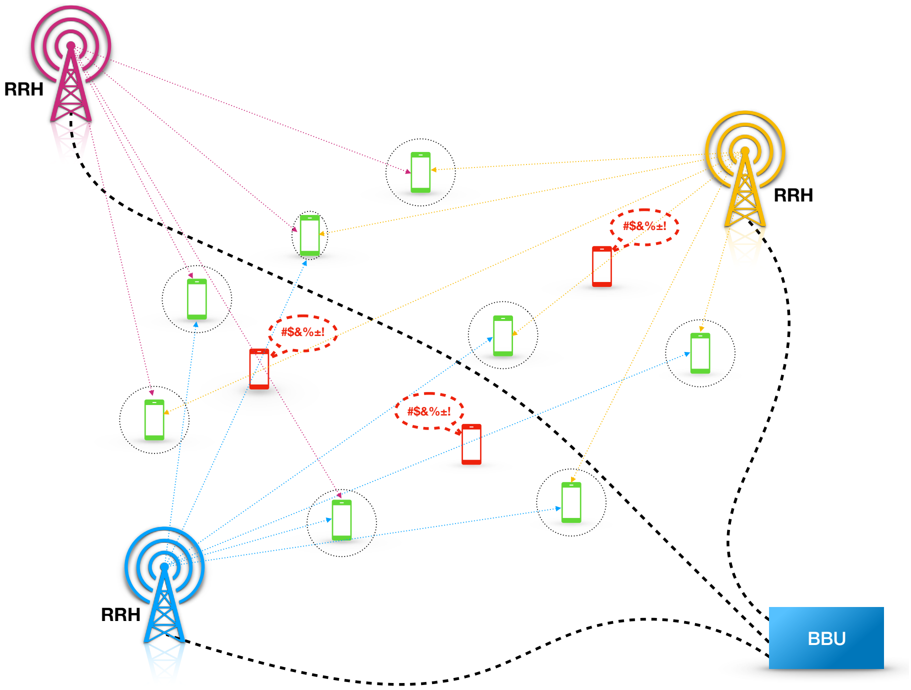


Figure 3.10: Cooperative radio access network.

where B is the number of base-stations, g_i is the complex channel gain coefficient associated with the transmission of the i^{th} base-station, and τ_i is the corresponding delay. $s_{Conf}(t)$ is the confidential message intended for the legitimate user, and $z(t)$ is the additive Gaussian noise at the receiver.

On the other hand, at any other location the B signals will not be the same due to the directional modulation selectivity which inherently causes interference to all directions outside the information beams,

$$r_d(t) = \sum_{i=1}^{B} g_i(t-\tau_i)\mathbf{h}^{\dagger}(\theta_i)\mathbf{w}(t) + z(t). \tag{3.22}$$

Including the knowledge of CSI in the synthesis process of $\mathbf{w}(t)$ at the transmitter would further improve the secrecy performance as shown in previous sections. Allowing the base stations to divide the data into different components each transmitted from a different base station and taking into account pre-compensation of channel effects, the data can be distributed in such a way that the signals can be coherently added at the user's locations to compose the intended data. This division pattern is not unique and does not need to be known at the receiver. Hence, it can be changed continuously to further secure the transmission (i.e., the synthesis process of $\mathbf{w}(t)$ can be changed from one transmission block to another).

3.2.1.3 Vulnerable Region Evaluation

To quantify the location-specific security achieved against eavesdropping in the wireless system, we define a new security metric called the vulnerable region. For a network with M users, VR is defined as the average of the Vulnerable regions of all users in the network

$$VR = \frac{1}{M}\sum_{i=1}^{M} VR_i \tag{3.23}$$

where the vulnerable region of the i^{th} user VR_i is the region in which a receiver can decode the data of the i^{th} user. To test our scheme, we generate the location of users randomly within a 2-D grid served by B base stations. The number of users that can be served simultaneously, M, depends on the number of antenna array elements N. We consider the full capacity of the system by letting the number of users equal to the number of antenna array elements (i.e., $N = M$). We divide the area of the network into K square points. Hence, the number of squares in which the information of legitimate users is accessible normalized to the total points of the network gives the vulnerable region metric. We consider the signal at a location to be decodable when the bit error rate (BER) reaches a certain threshold η.

$$VR_i = \frac{1}{K}\sum_{k=1}^{K} U\left(\eta - BER_k\right) \tag{3.24}$$

where $U(.)$ is the unit step function. The threshold η and the ratio between k and the total area of the covered grid can be chosen based on the secrecy requirement of the system.

3.2.2 Signal Structure

We define matrices $\mathbf{A} = \{\alpha_{ml}\}_{M\times L}$ and $\mathbf{H} = \{\mathbf{h}(\theta_l)\}_{1\times L}$. With the availability of $\mathbf{A}$ and $\mathbf{H}$ at the base station, the transmitted antenna pattern can be synthesized as

$$f(\theta,k) = \mathbf{h}^\dagger(\theta)\mathbf{H}[\mathbf{H}^\dagger\mathbf{H}]^{-1}\mathbf{A}^\dagger[\mathbf{A}\mathbf{A}^\dagger]^{-1}\mathbf{x}(k) = \mathbf{h}^\dagger(\theta)\mathbf{D}\mathbf{x}(k), \tag{3.25}$$

where $\mathbf{x} \in \mathbb{C}^{M\times 1}$ vector that contain the users data. Then, the SINR for the m^{th} transmitted signal $x_m(k)$ at any arbitrary direction θ can be calculated using (3.10), with $\mathbf{D} = \mathbf{H}[\mathbf{H}^\dagger\mathbf{H}]^{-1}\mathbf{A}^\dagger[\mathbf{A}\mathbf{A}^\dagger]^{-1}$.

We can see from (3.25), that the transmitted pattern at any direction θ is a linear combination of all M data streams. Then, if an eavesdropper is trying to decode the m^{th} message based on the reception of a single direction, it will suffer from a high interference level due to the other $M-1$ streams. We will show later that the received SIR value has a high probability of being low.

3.2.2.1 Eavesdropper with a Single Antenna

Based on this model, the received signal at any receiver in the network is given as

$$r(k) = \mathbf{e}\tilde{\mathbf{H}}^\dagger\mathbf{D}\mathbf{x}(k) = \mathbf{v}\times\mathbf{x}(k), \tag{3.26}$$

where $\mathbf{e} = \{\varepsilon_q\}_{1\times Q}$, ε_q is the complex gain of the q^{th} received path, and Q is the total number of received paths. $\tilde{\mathbf{H}} = \{\mathbf{h}(\theta_q)\}_{1\times Q}$ is the steering matrix corresponding to the transmission directions θ_q with $q \in \{1,2,\ldots,Q\}$.

Then, considering the decoding of the m^{th} message, the received SINR can be calculated as

$$\gamma^n = \frac{|v_m|^2\,\sigma_m^2}{\sum_{j\neq m}|v_j|^2\sigma_j^2+\sigma_{n_m}^2}, \tag{3.27}$$

where v_j is the j^{th} element of $\mathbf{v}$ which represent coefficient affecting the data of the j^{th} user. For the m^{th} legitimate user $\{\mathbf{e} \equiv \mathbf{a}_m, \tilde{\mathbf{H}} \equiv \mathbf{H}\}$, where $\mathbf{a}_m$ is the m^{th} row of $\mathbf{A}$ representing the channel of the mth user. This will result in,

$$\begin{aligned} \mathbf{v} &= \mathbf{a}_m \mathbf{H}^\dagger \mathbf{D}, \\ &= \mathbf{a}_m \mathbf{H}^\dagger \mathbf{H}[\mathbf{H}^\dagger \mathbf{H}]^{-1} \mathbf{A}^\dagger [\mathbf{A}\mathbf{A}^\dagger]^{-1}, \\ &= \mathbf{a}_m \mathbf{A}^\dagger [\mathbf{A}\mathbf{A}^\dagger]^{-1}, \end{aligned} \tag{3.28}$$

This leaves us with,

$$\begin{aligned} v_m &= 1, \\ v_{j \neq m} &= 0, \\ \gamma^m_{\text{Legit}} &= \sigma^2_m / \sigma^2_{n_m}. \end{aligned} \tag{3.29}$$

Otherwise, if there is a mismatch between the channel used at the transmitter and the actual channel, the legitimate receiver will experience some multi-user interference. The effect of multi-user interference on the secrecy performance will be discussed in subsection E.

In the case of an eavesdropper $\{\mathbf{e} \equiv \mathbf{b}, \mathbf{v} = \mathbf{b}\tilde{\mathbf{H}}^\dagger \mathbf{D}\}$, where $\mathbf{b} = \{\beta_p\}_{1 \times P}$. The received SINR for that case would be,

$$\gamma^m_{\text{Eaves}} = \frac{|\mathbf{b}\tilde{\mathbf{H}}^\dagger \mathbf{d}_m|^2 \sigma^2_m}{|\mathbf{b}\tilde{\mathbf{H}}^\dagger \mathbf{D}_m|^2 \sigma^2_{int} + \sigma^2_{n_e}} \tag{3.30}$$

where $\mathbf{d}_m$ is the m^{th} column of $\mathbf{D}$, representing the precoding vector for the m^{th} data stream. $\mathbf{D}_m$ is the rest of the precoding matrix $\mathbf{D}$ after removing $\mathbf{d}_m$. σ^2_{int} is the transmission power associated with the $M-1$ interfering streams, and $\sigma^2_{n_e}$ is the noise power at the eavesdropper side.

In order to consider the minimum guaranteed secrecy, we assume that the eavesdropper has a noiseless channel (i.e., $\sigma_e^2 = 0$)[5]. Then, the achievable secrecy rate can be defined as,

$$\begin{aligned} R_m &= R_l - R_e, \\ &= \left[\log_2(1+\gamma^m_{\text{Legit}}) - \log_2(1+\gamma^m_{\text{Eaves}})\right]^+ . \end{aligned} \tag{3.31}$$

The performance of the system in term of average achievable secrecy rate and secrecy outage probability will be investigated in the next section. Consider theorem 1 for the distribution of γ^m_{Legit} and R_e.

Theorem 1. *The achievable rate at the eavesdropper follows a Logistic distribution, $Logistic(\log(\frac{\mathscr{P}}{\sigma^2_{int}}), \frac{1}{M})$, hence, the received SINR follows a Shifted-Log-Logistic distribution.*

Proof. Starting from (3.28), with the assumption of i.i.d. elements of $\mathbf{A}$ and the large number of antenna elements N, it is valid to assume that the elements of the resulting vector $\mathbf{v}$ are complex Gaussian random variables according to the central limit theorem ($v_j \sim CN(0,1)$).

For the proposed system to serve K users, at least $(N > K)$ antenna elements are needed. The number of involved users K, not the number of antennas N, is the main determinant for the performance of the system. The assumption of a large number of antennas is made in order to assure that the system is able to serve a large enough number of users. With larger number of users involved, the central limit theorem assumption is justified. On the other hand, when a limited number of users is present, we can see that there is a mismatch between the simulation and theoretical results, which appears in Figure 3.14. This would make the squared magnitude follows an exponential distribution ($|v_j|^2 \sim Exp(\lambda)$), with the shape parameter $\lambda = 1$.

Considering the worst case where the eavesdropper channel is noiseless ($\sigma^2_{n_e} = 0$), we can rewrite (3.30) as,

$$\gamma^m_{\text{Eaves}} = \frac{|\mathbf{b}\tilde{\mathbf{H}}^{\dagger}\mathbf{d}_m|^2\sigma_m^2}{|\mathbf{b}\tilde{\mathbf{H}}^{\dagger}\mathbf{D}_m|^2\sigma_{int}^2} \tag{3.32}$$

[5] The assumption of noiseless eavesdropper channel corresponds to calculating a lower bound on performance.

Letting $X = |\mathbf{b}\tilde{\mathbf{H}}^{\dagger}\mathbf{d}_m|^2$, $Y = |\mathbf{b}\tilde{\mathbf{H}}^{\dagger}\mathbf{D}_m|^2$, and $Z = X + Y$, the eavesdropper achievable rate would be,

$$\begin{aligned} R_e &= \log(1+\frac{X\sigma_m^2}{Y\sigma_{int}^2}) \\ &= \log(\frac{Z\mathscr{P}}{Y\sigma_{int}^2}) \\ &= \log(\frac{\mathscr{P}}{\sigma_{int}^2}) - \log(\frac{Y}{Z}) \end{aligned} \tag{3.33}$$

with Y and Z following the exponential distribution $Exp(1)$. Then, the received SINR will take the form,

$$\gamma_{\text{Eaves}}^m = \frac{\sigma_{int}^2\, e^{(R_e-\mu)}}{\mathscr{P}} - 1. \tag{3.34}$$

The formula in (3.33) resembles a random variable with a Logistic distribution, $Logistic(\mu,\beta)$. where $\mu = \log(\frac{\mathscr{P}}{\sigma_{int}^2})$ is the location parameter, and $\beta = 1/M$ is the scale parameter,

$$F_{R_e}(r) = 0.5\left[1+\tanh\left(\frac{r-\mu}{2\beta}\right)\right], \tag{3.35}$$

Moreover, The received SINR γ_{Eaves}^m would follow the Shifted-Log-Logistic distribution with parameters $\alpha = e^{\mu} - 1$, $\sigma = Me^{-\mu}$, and $\varepsilon = \mu$. Then, the CDF of the SINR is given as,

$$F_{\gamma_{\text{Eaves}}^m}(\gamma) = \frac{1}{1+\left(1+\frac{\varepsilon(\gamma-\alpha)}{\sigma}\right)^{-\frac{1}{\varepsilon}}}. \tag{3.36}$$

Hence, the secrecy outage probability can be calculated as,

$$\begin{aligned} P(R_m \leq \gamma_{th}) &= P\left[(R_l - \gamma_{th}) \leq R_e\right] \\ &= 1 - F_{R_e}(R_l - \gamma_{th}). \end{aligned} \tag{3.37}$$

□

Here, the eavesdropper is considered entirely passive, and the information about its channel is not available to any of the legitimate users. As part of the performance evaluation, it will be compared to the performance of MIMO precoding with AN, while considering the optimal power distribution between data and AN [62].

3.2.2.2 Eavesdropper with an Arbitrary Number of Antennas

The case of an eavesdropper with multiple receiving antennas can be thought of as equivalent to a network with multiple eavesdroppers. It represents the worst-case scenario of the multiple-eavesdroppers case, where all the eavesdroppers have perfect cooperation channel. On the other hand, it must be noted that the scenarios studied in the sequel do not consider the cases of active eavesdroppers.

Considering the AN system, and due to the aforementioned assumption of the availability of **A** at the eavesdropper, the eavesdropper can reconstruct the pre-coding matrix on its side. For the case where $\{N_E < N_A\}$, the eavesdropper will not be able to separate the legitimate data from the noise components. When $\{N_E \geq N_A\}$ and assuming knowledge of the pre-coding matrix, the eavesdropper has enough information to be able to extract the legitimate data from the noise imposed over it [63]. Here, N_A represents the number of antennas at the transmitter of the AN scheme, which corresponds to M in our proposed scheme.

Redefine the received signal at the eavesdropper as,

$$\mathbf{r}_e(k) = \mathbf{B}\tilde{\mathbf{H}}^{\dagger}\mathbf{D}\mathbf{s}(k), \tag{3.38}$$

where $\mathbf{B} = \{\beta_{np}\}_{N_E \times P}$ and β_{np} represents the gain coefficient of the p^{th} path received by the n^{th} antenna.

For the AN case, the pre-coding matrix **D** is constructed using only statistical information of the channel. This information is fed back to the transmitter, which makes it vulnerable to the eavesdropper. In such case, as stated earlier, the eavesdropper can reconstruct **D** and acquire the transmitted data if it has enough receiving antennas.

For the proposed scheme, and based on equation (3.38), the transmission directions, embedded in **H**, goes into the construction of the precoding matrix **D**. **H** is assumed to be exclusively known at the base station[6]. Due to the lack of knowledge of **H** at the eavesdropper side, it will not be able to perfectly reconstruct **D** and extract the legitimate data, even for the case where $\{N_E \geq M\}$. Later, we will also show that the random generation of **H** will not be beneficial, in order to correctly extract the legitimate data.

3.2.2.3 Multiple Access Secrecy Rate

Another concern, for the multiple access systems, is the secrecy sum-rate. The secrecy sum-rate is calculated based on the amount of data leaked from one user to the other users in the system. The achievable secrecy sum-rate is obtained by considering the worst-case scenario, where for each legitimate user m the remaining $M-1$ users are considered as collaborative eavesdroppers [64]. This case is equivalent to a multi-input, single-output, multi-eavesdropper (MISOME) wiretap channel [30]. The achievable secrecy sum-rate R_{sum} is given by,

$$R_{sum} = \sum_{m=1}^{M} \left[\log_2(1+\gamma_m) - \log_2(1+\gamma_{\hat{m}})\right]^+ \tag{3.39}$$

by replacing **b** with $\mathbf{a_m}$ in equation (14) and based on [64], we can define,

$$\gamma_m = \frac{|\mathbf{a}_m \mathbf{H}^\dagger \mathbf{d}_m|^2}{\sum_{j \neq m} |\mathbf{a}_m \mathbf{H}^\dagger \mathbf{d}_j|^2 + \sigma_{n_m}^2}, \tag{3.40}$$

$$\gamma_{\hat{m}} = ||\mathbf{A}_m \mathbf{H}^\dagger \mathbf{d}_m||^2 \tag{3.41}$$

[6] The estimation process of the directions used for transmission and the generation of the steering vectors are exclusively done at the base-station. This information is not shared at any point during the communication process. This makes it not possible for the eavesdropper to acquire such information.

where $\mathbf{A}_m$ is the rest of $\mathbf{A}$ after removing $\mathbf{a}_m$, and $\mathbf{d}_j$ is the part of the pre-coder related to the j^{th} user data.

Basically, γ_m represents the power of the m^{th} legitimate message at the m^{th} user compared to the interference imposed on it from the rest $M-1$ messages. While $\gamma_{\hat{m}}$ represents the leakage of the m^{th} message received by the remaining $M-1$ users.

In the proposed system, the pre-coder zero-forces the M legitimate messages with respect to each other. This means that in the event of perfect knowledge of the users CSI's, the sum rate would be infinite. For more realistic assumption, in the next section, we will consider the case of imperfect CSI knowledge and study its effect on the achievable secrecy sum-rate.

3.2.2.4 Power Allocation

The work in this paper focuses on studying performance evaluation and simulation under equal power allocation, where all transmitted streams are allocated the same power. While this strategy might not result in the optimal system performance, it enables simplicity in terms of practical system implementation as well as tractability in terms of mathematical analysis. The results obtained here can be thought of as a lower bound on the optimal system performance.

The system can be further extended to incorporate different power allocations for different directions which will require further studies into different power allocation strategies as well which is left as a future expansion of this work. Here, we are discussing some of the other applicable power allocation strategies. Since the secrecy aspects are the main drive for this work, the focus should be on utility functions such as secrecy rate and secrecy outage probability. Then, the optimization problems can be formulated as follows,

$$\begin{aligned}
\{\sigma_1^2,\sigma_2^2,\ldots,\sigma_M^2\} &= \arg \max_{\sigma_1^2,\sigma_2^2,\ldots,\sigma_M^2} R_{sum} \\
\{\sigma_1^2,\sigma_2^2,\ldots,\sigma_M^2\} &= \arg \max_{\sigma_1^2,\sigma_2^2,\ldots,\sigma_M^2} \bar{R}_s \\
\{\sigma_1^2,\sigma_2^2,\ldots,\sigma_M^2\} &= \arg \min_{\sigma_1^2,\sigma_2^2,\ldots,\sigma_M^2} P(\bar{R}_s < \gamma_{th})
\end{aligned} \tag{3.42}$$

where $\bar{R}_s = \frac{1}{M}\sum_{i=1}^{M} R_i$ is the average achievable secrecy rate per user. Besides, based on the desired application, various constrains can be imposed on the system. Exemplary constraints may include, but not limited to, total power ($\sum_{m=1}^{M} \sigma_m^2 \leq \mathscr{P}$), average power, average received SINR per user, or enhancing the overall fairness between users.

3.2.3 “Secret-Sharing” Based Enhanced Secrecy

In order to further enhance the secrecy performance of the system, a cryptography based approach can be incorporated in the proposed signal structure. First we will provide a overview of the cryptography approach called *secret sharing*. Then, the approach of applying it to the current signal structure will be discussed. The enhanced performance will be presented in the next subsection with the rest of the performance results.

3.2.3.1 Secret Sharing

In [65,66], Blakley and Shamir respectively introduced a secure algorithm to share a secret message. The scheme we are adopting is the (B,L)-threshold scheme, where $(B \leq L)$, and B,L are positive integers. A secret $\mathscr{X}$ can only be retrieved if at least B participants out of the available L were able to collaborate with their respective shares.

This scheme is recently introduced as a mean to securely transfer visual and acoustical content [67,68]. The dealer $\mathscr{D}$, which has the knowledge about the secret message $\mathscr{X}$, selects $(B-1)$ random elements denoted $\mathbf{a} = [a_0, a_1, \ldots, a_{(B-1)}]^T$, while $a_0 = \mathscr{X}$. $\mathscr{D}$ uses $\mathbf{a}$ as the coefficients to generate a polynomial of the order B Then, $\mathscr{D}$ computes the L shares, which are the values of the generated polynomial, as,

$$y_i = \sum_{j=0}^{B-1} a_j v_i^j \mod p \qquad \forall i \in \{1,2,\ldots,L\} \tag{3.43}$$

where each v_i is a point on the polynomial and randomly selected, and $p > L$ is a prime to ensure that all operations are performed in a finite field.

If the participants are able to combine at least B shares, the secret $\mathscr{X}$ can be retrieved using one of the following approaches,

• *Solving a system of linear equations:*

$$\mathbf{a} = \mathbf{V}^{-1}\mathbf{y}, \tag{3.44}$$

where $\mathbf{y} = [y_1, y_2, \dots, y_B]^T$ and $\mathbf{V} = \{v_i^j\}_{B\times B}$ is a Vandermonde matrix and its determinant is given as,

$$\det\mathbf{V} = \prod_{1\leq i<j\leq B}(v_i - v_j) \quad \text{mod}\ p. \tag{3.45}$$

As all v's are distinct, there are no zero terms in the product, and hence, $\det V \neq 0$. Therefore, the system has a unique solution.

• *Using Lagrange interpolation:*

$$\mathscr{X} = \sum_{i=1}^{B} y_i \cdot c_i, \tag{3.46}$$

where

$$c_i = \prod_{\substack{j=1\\ j\neq i}}^{B} \frac{v_j}{v_i - v_j}. \tag{3.47}$$

The value of $c_i, \forall i \in [l]$ can be pre-computed, and considered publicly accessable.

For the case of $(B = L)$, the secret retrieval can be reduced to,

$$\mathscr{X} = \sum_{i=1}^{B} y_i. \tag{3.48}$$

3.2.3.2 Signal Construction

The proposed algorithm requires a number of sources B, each of these sources transmits one of the possible $y_m^{(i)}$ shares, which are generated based on the secret message of the m^{th} user. The sources then directionally modulate these shares to the predefined location of the m^{th} user x_m. Once the signals from all sources are added together at the location of the m^{th} user, the receiver can correctly decode the secret message. In such case, an eavesdropper that is geographically located in a different place, other than the legitimate receiver, cannot successfully decode the message as it is unable to collect all the fragments of the secret.

Although the proposed algorithms is applicable for different system structures, we adopt the CoMP based structure [60] as a way to prove the concept. Some other possible system structures that would benefit from such algorithms are, a single base-station in a multi-tap environment, where the signal can reach the user through different communication paths each of them carrying a different fragment of the secret. Another system would be a relay based network, where we can solve the untrusted relay problem by limiting the availability of information at the relays to only the non-reconstructable fragments.

The adopted system consists of B transmission points (TP), and each TP is equipped with a ULA of length N. The system serves M users, each user is equipped with a single omni-directional antenna. We assume that all eavesdroppers in the system are passive, which makes the system unaware of their CSI. The received signal at any location is given by,

$$\begin{aligned} r(k) &= \sum_{i=1}^{B} g^{(i)}(k-\tau_i)s^{(i)}(\theta,k)+z(k), \\ &= \sum_{i=1}^{B} g^{(i)}(k-\tau_i)\mathbf{h}^H(\theta^{(i)})\mathbf{w}^{(i)}(k)+z(k). \end{aligned} \tag{3.49}$$

where $g^{(i)}$ is the channel gain coefficient associated with the transmission of the i^{th} base-station, and τ_i is the corresponding delay. $s^{(i)}$ is the transmitted signal, and $z(t)$ is the additive Gaussian noise at the receiver. For simplicity, we assume full synchronization, where the signals of all TPs arrive at the appropriate time at the desired location (i.e., $\tau_i = \tau \quad \forall i$).

Then, the weights vector of the i^{th} TP is given as,

$$\mathbf{w}^{(i)}(k) = \mathbf{H}\left(\mathbf{H}^H\mathbf{H}\right)^{-1}\mathbf{y}^{(i)}(k), \tag{3.50}$$

where $\mathbf{y}^{(i)}(k) = \left[y_1^{(i)}(k), y_2^{(i)}(k), \ldots, y_M^{(i)}(k)\right]^T$ are the shares of the M legitimate users, given to the i^{th} TP. We assume that each TP has a power constraint of P_i, then $\left(\sum_{m=1}^{M}\alpha_m \leq \sum_{i=1}^{B}P_i\right)$.

With such a structure of weights, the signal received at the location of any of the M users can be described as,

$$\begin{aligned} r_m(k) &= \sum_{i=1}^{B} g^{(i)}(k)\mathbf{h}^H(\theta^{(i)})\mathbf{H}\left(\mathbf{H}^H\mathbf{H}\right)^{-1}\mathbf{y}^{(i)}(k) + z(k), \\ &= \sum_{i=1}^{B} g^{(i)}(k)y_m^{(i)}(k) + z(k) = x_m(k) + z(k). \end{aligned} \tag{3.51}$$

For any other location, the receiver won't be able to retrieve the message due to the following,

- Directional Modulation effect: where all the information outside the main beam is randomized.
- Secret sharing effect: even if the eavesdropper is in line with the main beam of one of the BSs, it will not be able to collect the other pieces of the secret unless it is co-located with the legitimate user.

Moreover as the polynomial coefficients **a** are selected randomly, there is no fixed pattern, for the transferred secrets, that the eavesdropper is able to trace (i.e., the system is dynamic).

3.2.3.3 Secrecy Analysis

For simplicity we will adopt an (B,B)-threshold algorithm, so that the secret is directly recovered by adding all the shares, which is also suitable for wireless environment as the signals are directly superimposed over the air.

Construction 1. *For any set of secrets $\mathscr{X} \in \mathbb{C}^M$, the encoder/decoder pair can be represented as,*

$$\begin{aligned} Enc(x_m) = y_m^{(i)} &= \left(\frac{x_m}{B} + a_i - \frac{1}{B-1}\sum_{j\neq i} a_j\right)_{\forall i\in[B]}, \\ Dec(\mathbf{y}_m) &= \sum_{i=1}^{B} g^{(i)} y_m^{(i)} = x_m, \end{aligned} \tag{3.52}$$

where a_i is an arbitrary complex number chosen based on the Gaussian distribution $\mathcal{N}(0,1)$.

It was proven in [69] that, for any subset of shares $\hat{\mathbf{y}}_m$ where $|\hat{\mathbf{y}}_m| < B$, a scheme following Construction 1 is δ_B-secure, where,

$$\delta_B = \mathbb{I}\left[\mathscr{S}_m(k); \hat{\mathbf{y}}_m(k)\right] \leq \frac{2(B-1)}{B}. \tag{3.53}$$

Based on the data-processing inequality [70], this result acts as the upper limit on the information transferred to the eavesdropper, which is not able to collect all the shares,(i.e., $\mathbb{I}[\mathscr{S}_m(k); r(k)] \leq \mathbb{I}[\mathscr{S}_m(k); \hat{\mathbf{y}}_m(k)]$). This is the typical situation for the suggested system, where the eavesdropper will not be able to retrieve all the shares unless it is physically co-located with the legitimate user. An extreme case where the eavesdropper is able to collect all the shares would be if there is a single legitimate user and B cooperative eavesdroppers. We are proposing a modified scheme to avoid such situation in the next section.

Considering the worst case scenario, where the eavesdropper has a noiseless system, and does not receive interference from the shares of the other $M-1$ users. Then the lower bound on the achievable secrecy rate is given as,

$$\begin{aligned} R_s^{(m)} &= R_l - R_e \\ &= \mathbb{I}\left[\mathscr{S}_m(k); r_m(k)\right] - \mathbb{I}\left[\mathscr{S}_m(k); r_e(k)\right] \\ &= \log_2(1+\frac{\alpha_m}{\sigma_z^2}) - \log_2(1+\gamma_e) \end{aligned} \tag{3.54}$$

and the received SINR at the eavesdropper is,

$$\gamma_e = \frac{\sum_{i=1}^{\hat{B}} \frac{|l^{(i)}|^2\alpha_m}{B|g_m^{(i)}|^2}}{\sum_{i=1}^{\hat{B}} \frac{(B-1)|l^{(i)}|^2\alpha_m}{B|g_m^{(i)}|^2} + \sum_{i=\hat{B}+1}^{B} \frac{|l^{(i)}|^2\alpha_{j\neq m}}{|g_{j\neq m}^{(i)}|^2} + \sigma_e^2} \tag{3.55}$$

where $\hat{B}$ is the cardinality of $\hat{\mathbf{y}}$, and $l^{(i)}$ is the channel gain between the eavesdropper and the i^{th} base-station. The denominator of (3.55) can be explained as follows, the first term represents the interference due to the insufficient number of collected shares, The second term is the interference from the shares that are not related to the m^{th} secret, and σ_e^2 is the noise power. While the nominator represent the amount of leakage about the m^{th} secret.

As we proved in [52], the secrecy outage probability of such system can be given as the CCDF of a logistic random variable (i.e., $R_e \backsim Logistic(\mu,\beta)$). If we consider an eavesdropper with a noiseless channel ($\sigma_e^2 = 0$), and an equal power distribution for all users, for simplicity, ($\alpha_m = \alpha, \forall m \in [M]$), we get,

$$\mu = log_2(\frac{B^2}{B^2-\hat{B}^2}) \qquad \beta = \frac{\hat{B}}{B^2}, \tag{3.56}$$

and

$$\begin{aligned} Pr(R_s \leq \gamma_{th}) &= 1 - F_{R_e}(R_l - \gamma_{th}) \\ &= 0.5\left[1 - \tanh\left(\frac{R_l - \gamma_{th} - \mu}{2\beta}\right)\right] \end{aligned} \tag{3.57}$$

where γ_{th} is a predefined secrecy rate threshold.

On another perspective, the number of antenna array elements N does not directly affect the secrecy rate or outage performance. Increasing the number of the elements would results in the ability to have a narrower information beam, which would reduce the area where transmitted shares are accessible, also the area where the secret is detectable. Moreover, increasing the number of element s will allow the system to serve a larger number of users.

3.2.4 Secrecy Performance

Here, we assume that the entries of $\mathbf{A}$ and $\mathbf{B}$ are independently identically distributed (i.i.d.) and they follow a complex Gaussian distribution with zero mean and a unit variance. Moreover, $\mathbf{A}$ and $\mathbf{B}$ are totally uncorrelated, which is a valid assumption unless the legitimate user and the eavesdropper are co-located.

For our system performance results, , all users are assumed to be assigned an equal transmission power, $\sigma_j^2 = \frac{\mathscr{P}}{M}, \forall j \in \{1, 2, \ldots, M\}$. The analysis of the power allocation for each user is not considered for this work. Also, the channel of the eavesdropper is always assumed to be noiseless $\sigma_{n_e}^2 = 0$ as a secrecy worst-case scenario.

3.2.4.1 Eavesdropper with a Single Antenna

Fig. 3.11 shows the complementary cumulative distribution function (CCDF) of $\gamma(\theta)$ from (3.10), with a precoding matrix $\mathbf{D} = \mathbf{H}[\mathbf{H}^\dagger\mathbf{H}]^{-1}\mathbf{A}^\dagger[\mathbf{A}\mathbf{A}^\dagger]^{-1}$. It shows that with a very high probability, the power of the interfering streams will be much larger than the power of the desired stream (i.e., $P\{\gamma(\theta) < 0 \text{ dB}\}$).

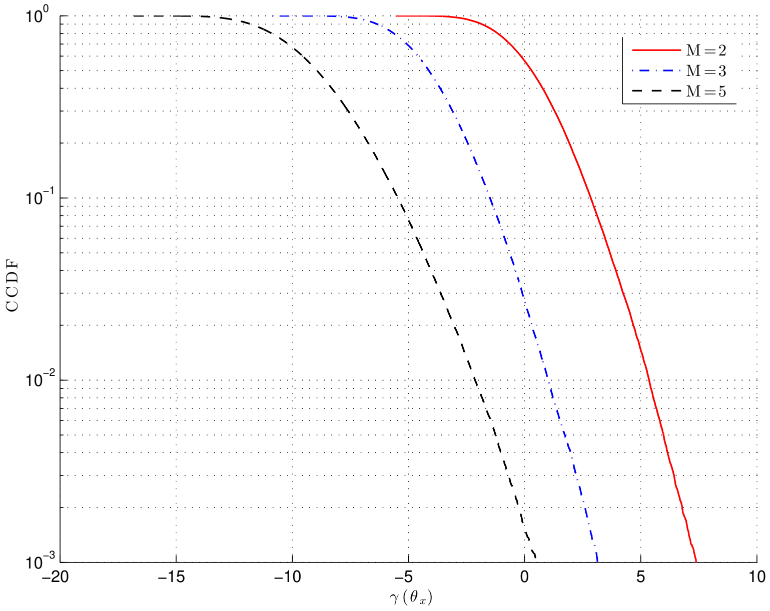


Figure 3.11: CCDF of the received SIR. the CCDF curve of the received SIR from a single path at any random transmission direction θ_x.

These results induce that the eavesdropper's channel has lower capacity than the legitimate user's channel. Notice that the effect of the noise at the eavesdropper is not considered in these results, which makes it the best case scenario for the received SINR.

It can be directly inferred that with the increase in the number of users in the system, the received SINR drops dramatically. The same analysis was carried for the received SINR at the eavesdropper, γ^m_{Eaves}, expressed by (3.30). In Fig. 3.12, the eavesdropper's channel suffers from high degradation with a high probability[7].

[7] Here, we refer to the degradation of the channel as the decrease happens to the value of the received SINR.

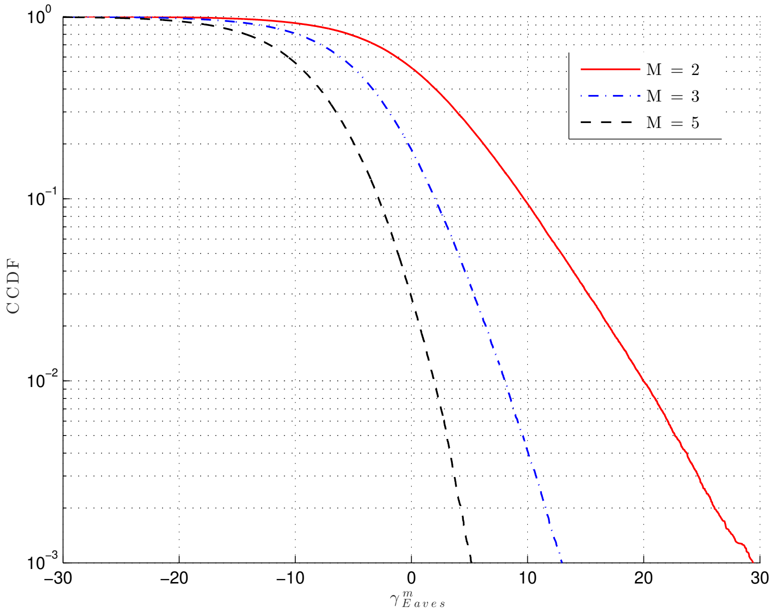


Figure 3.12: CCDF of the received SINR by the eavesdropper.

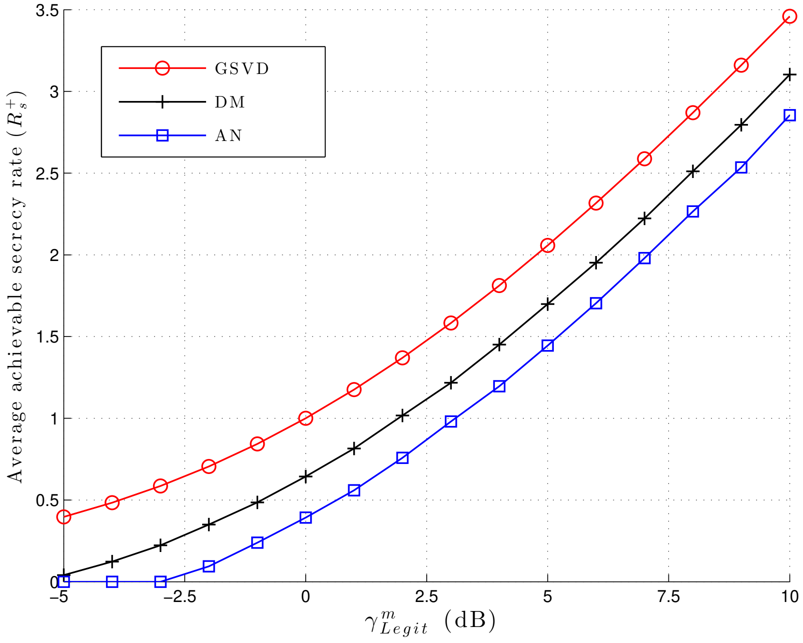


Figure 3.13: The change of the average achievable secrecy rate. (R_m) vs. the SNR of the legitimate user's channel (γ^m_{legit}).

Fig. 3.13 shows the change of the average achievable secrecy rate expressed by (3.27), with the change of the SNR at the legitimate user $\gamma^{m}_{\text{Legit}}$. Here, we compare three different schemes of secrecy namely, GSVD [31], DM, and AN. GSVD is know to achieve the secrecy capacity in case of full channel knowledge. We can see that the proposed scheme can achieve a secrecy rate closer to that of the GSVD, compared to the achievable rates when using the AN scheme.

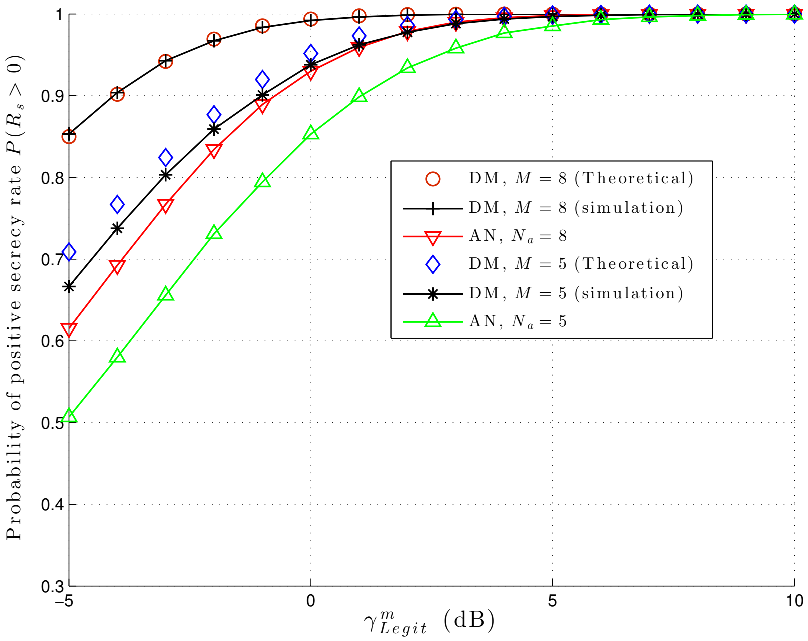


Figure 3.14: The probability of achieving a positive secrecy rate. $P(R_m > 0)$ against the received SNR at the legitimate user, for different system configurations.

On the other hand, Fig. 3.14 compares the probability of achieving positive secrecy rates in the case of using DM, with the AN scheme from [62]. The figure shows that DM outperforms AN scheme. Also the figure shows the theoretical curves of the DM schemes based on Theorem 1. We can see that the simulations match the theoretical results. Besides, it can be inferred that after a certain number of transmit antennas N_a, the enhancement of the performance of the AN scheme is no more significant.

Note that, increasing the number of transmit antennas for AN adds hardware (the number of required RF chains) and processing complexity. While, for DM, increasing the number of users M adds processing complexity only and keeps the hardware unchanged.

Fig. 3.15 shows the effect of the correlation between the legitimate channel and the eavesdropper's channel. As channels are being more correlated, AN loses performance faster than DM. This indicates that DM is more immune to channel correlation.

Another aspect of comparison is the ability to provide higher secrecy requirements. It is clear from Fig. 3.16 that DM can provide better performance when there are higher secrecy requirements. The figure shows that when the minimum secrecy rate threshold γ_{th} increases, DM tends to keep a more stable performance compared to AN.

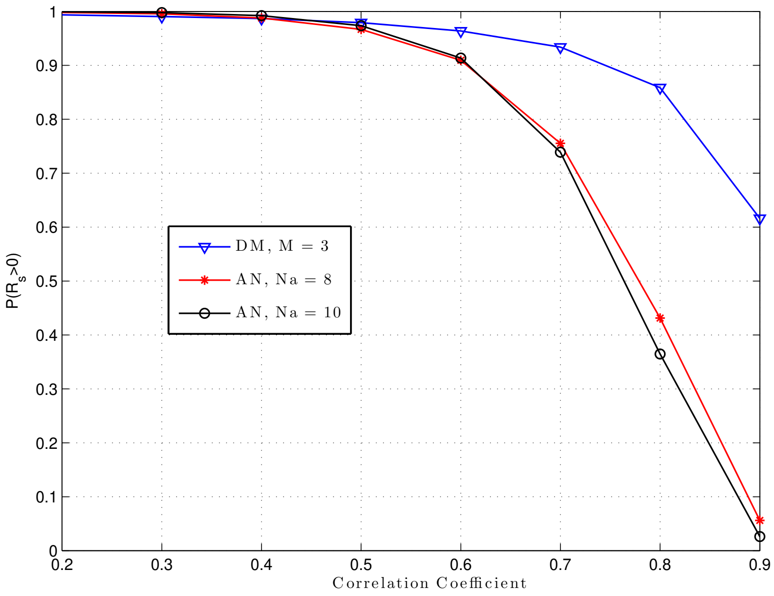


Figure 3.15: The effect of the channel correlation. the correlation between the channel of the legitimate user and the channel of the eavesdropper on achieving a positive secrecy rate $P(R_m > 0)$.

3.2.4.2 Eavesdropper with an Arbitrary Number of Antennas

As mentioned before, Due to the assumption of the availability of channel information of the legitimate users at the eavesdropper side, the eavesdropper can regenerate the pre-coding matrix and decode the legitimate data (for $N_E \geq M$) in the case of AN system. For our scheme, we add another component to the pre-coder, which is exclusively available at the base station.

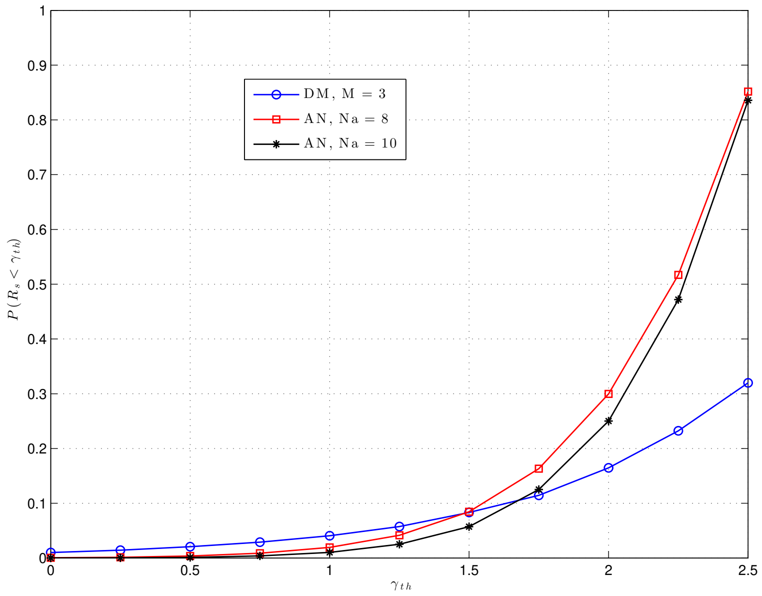


Figure 3.16: The secrecy outage probability. the probability for different secrecy requirements $P(R_m < \gamma_{th})$.

It is assumed that the eavesdropper has the knowledge about the structure of the antenna array used at the base station. This means it knows the general structure of the matrix **H**, but it is not aware of the values of θ_l.

Fig. 3.17 shows the probability of having positive secrecy rate for different number of antennas at the eavesdropper N_E. The proposed scheme can still achieve positive secrecy rate for an eavesdropper with large number of antennas, while the number of elements of the antenna array is fixed at $N = 10$.

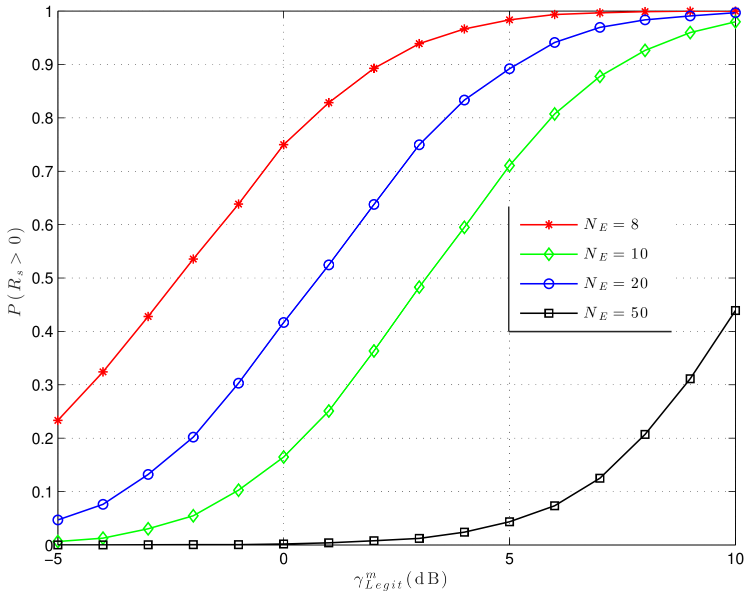


Figure 3.17: The probability of achieving positive secrecy rate. The rate for different number of antennas at the eavesdropper.

3.2.4.3 Multiple Access Secrecy Rate

As discussed before, in the case of perfect knowledge of the channel of each of the users, the pre-coder is capable of eliminating the effect of each signal on the other non-intended users. Here, we are showing the effect of channel estimation error on the secrecy performance. To be more practical, we adopted the channel estimation error model of the LTE system [71]. Fig. 3.18 shows the secrecy sum-rate against the channel estimation error, for different channel structures and different number of users. It is shown that the increase in the number of users in the system affects the secrecy rate.

This is due to the increase in the number of interfering signals that leak to the legitimate data. On the other side, having a more diverse channel helps to maintain some resistance against estimation error. The diverse channel helps to average the interference imposed on the legitimate signal, which is a zero-mean random variable.

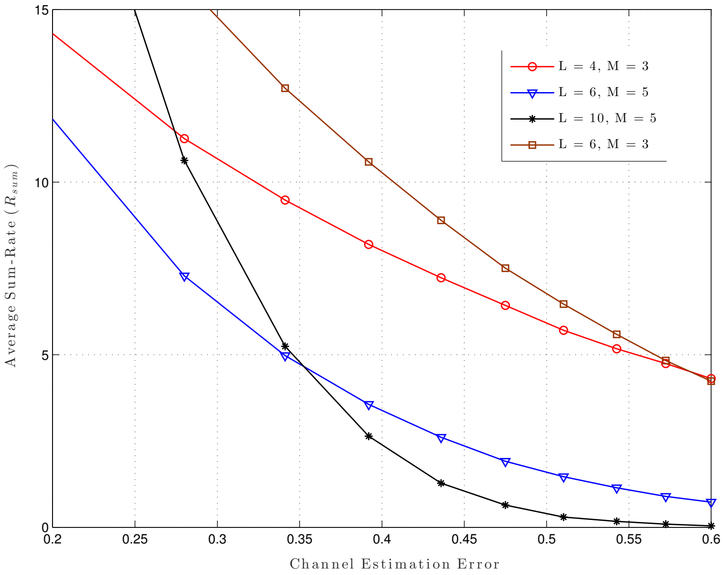


Figure 3.18: The Average secrecy sum-rate against the channel estimation error.

3.2.4.4 *Secrecy Using CoMP*

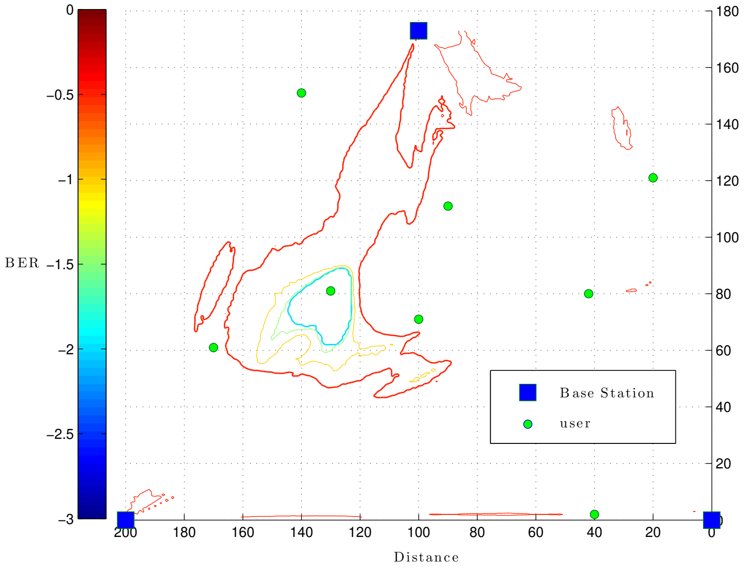


Figure 3.19: BER performance contour with 4-QAM and $N = 8$

The CoMP scheme requires the signal to be transmitted from several geographically separated base stations to provide security so that, along each direction of transmission, the data is not decodable. Here, we simulate a 100×100 area ($K = 10^4$) covered by 3 base-stations ($B = 3$). The number of users served in that area is based on the number of used antenna elements ($M = N = 8$). The secrecy threshold is chosen as $\eta = 10^{-2}$.

Fig. 3.19 shows the simulation of equally separated base stations. The base stations are configured such that the broadside direction of each antenna array is pointing towards the center of the equilateral triangular shape of the base stations positions. Using 4-QAM modulation scheme, contours of the noiseless BER performance for one of the users is shown where circles represent the users and squares are the base stations.

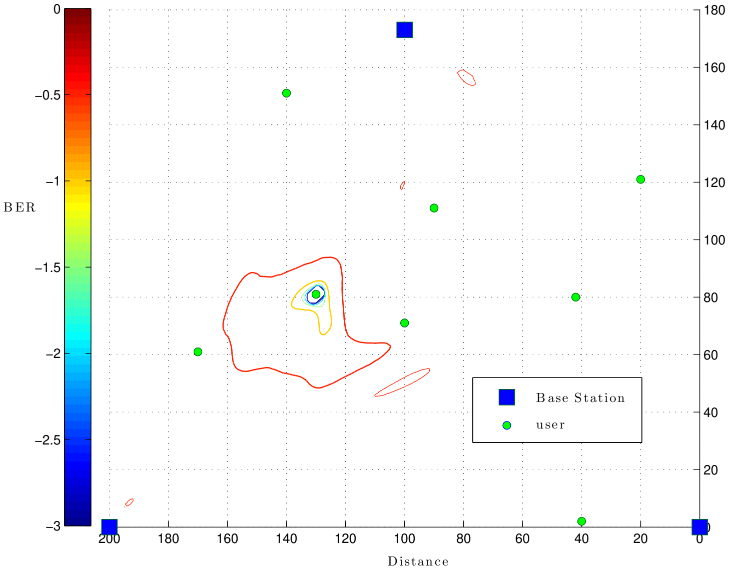


Figure 3.20: BER performance contour with 16-QAM and N=8

Fig. 3.20 shows the case where 16-QAM modulation is used. Notice how the secure region is reduced with increasing the modulation order. To further control the secure area, the number of activated antenna arrays elements is changed accordingly. Increasing the number of antenna elements narrows the information beam-width, reducing the vulnerable region as shown next.

In order to profile the performance of this location-specific security technique, we use the average VR metric to measure variations of the secure area. Fig. 3.21 shows the effect of varying the number of antenna elements of the base stations. It is clear that, for a given modulation order, as the number of elements increases, the VR reduces significantly. Furthermore, different modulation orders are simulated. As mentioned previously, higher modulation order allows for more confined VR. Hence, using both: antenna size and modulation order, full control over VR is attained.

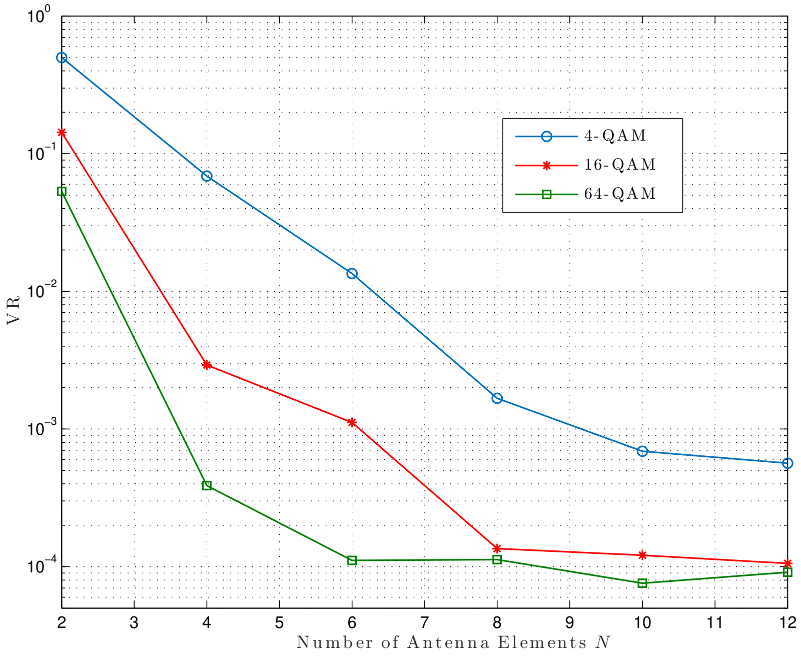


Figure 3.21: Vulnerable region reduction. The change with number of antenna elements for different modulation orders

3.2.4.5 "Secret-Sharing" Enhanced Performance

The system was simulated over a 50×50 grid with different number of sources (BSs). The system serves 5 users randomly located over the grid. The secrets consists of QPSK symbols. The channel gains $g_m^{(i)}$ are simulated for two cases, namely, free space fading and frequency selective channels. The location of the sources will be noted on the figures as blue squares. The area where the data is decodable is noted using black circles.

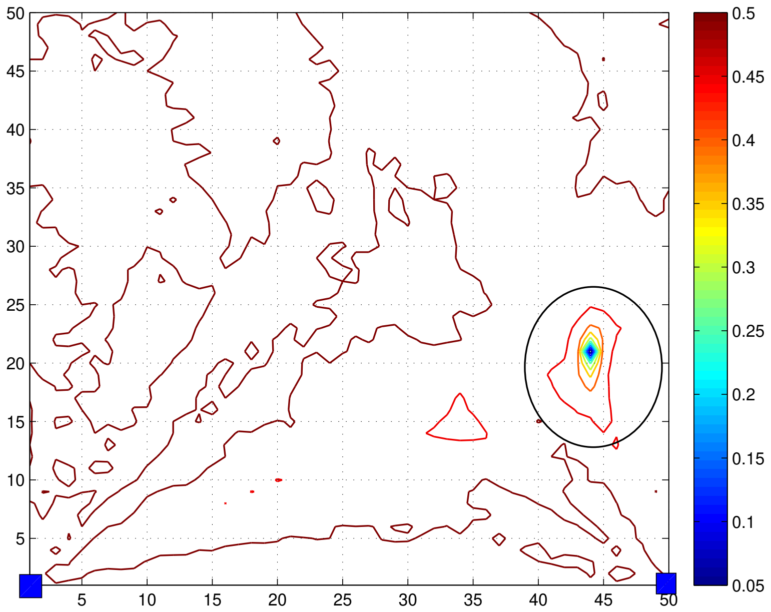


Figure 3.22: BER using two transmitters (case 1). BER for the data of one of the users at the location (44,22) [inside the black circle]. The secret is shared using two sources [the blue squares].

Figures 3.22 and 3.23 show the bit-error-rate (BER) values over the grid for two different users in the system. It is noticeable that the data is decodable in a very limited area around the location of the desired user, while outside that area the received symbols are almost random.

On the other hand, Figures 3.24 and 3.25 shows the magnitude of the correlation coefficient between the received signal and the shared secret calculated as,

$$\rho = \left| \frac{\mathrm{Cov}(r(k), \mathscr{S}_m(k))}{\mathrm{var}(r(k))\mathrm{var}(\mathscr{S}_m(k))} \right|. \tag{3.58}$$

The figures show that the received signal over the whole grid is almost uncorrelated with the shared secret, except for the area around the desired location. This confirms that the signal received outside the desired location does not have any form of linear relationship with the shared secret message.

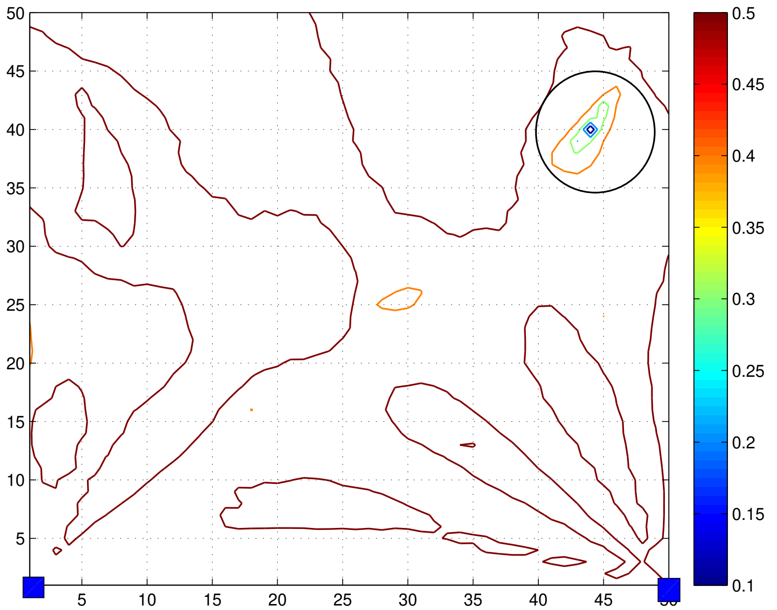


Figure 3.23: BER using two transmitters (case 2). BER for the data of one of the users at the location (44,40) [inside the black circle]. The secret is shared using two sources [the blue squares].

Figures 3.26, 3.27, 3.28, and 3.29 are similar to the previous figures, but instead of using only two sources to share the secret, Four sources are being used. The figures show that with the increase in the number of sources, the area where the message is decodable becomes much smaller. this can be used as a flexible option based on the secrecy requirements of each user.

Figure 3.30 shows the effect of including channel precoding, in case of a frequency selective channel. In such case, it is visible that the area where the data is decodable is much small, and the data received outside the desired location is more randomized.

Figure 3.31 shows the case of a system serving a single user. Even though the area of detectability is larger, the system is still able to provide secrecy over the most of the other areas. This elements the possibility that the system relies on multi-user interference only.

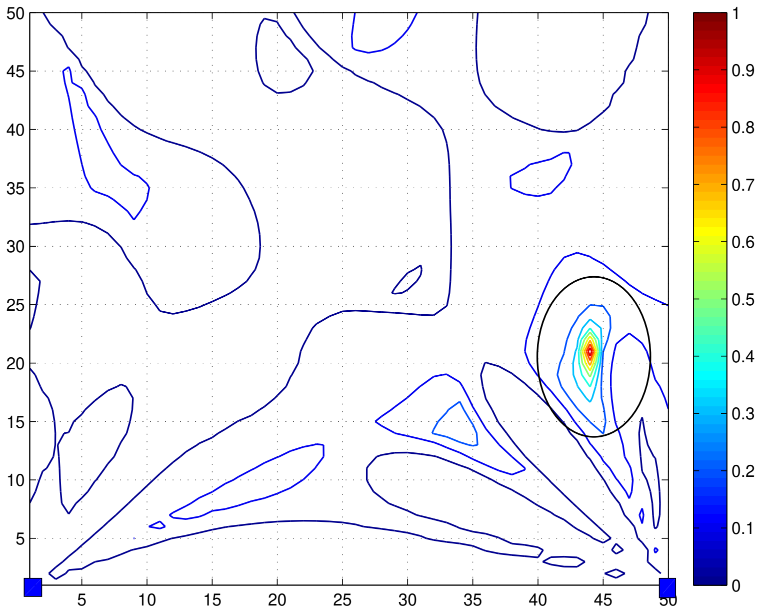


Figure 3.24: Signal correlation using two transmitters (case 1). The magnitude of correlation coefficient for the data of one of the users at the location (44,22) [inside the black circle]. The secret is shared using two sources [the blue squares].

Figure 3.32 shows the performance of the system without applying secret sharing scheme. This figure is provided as a reference for performance. We can see that the area surrounding the desired location is larger. Moreover, The locations along the line of sight of the source are all vulnerable.

Figure 3.33 shows the secrecy outage probability of the system with a secrecy threshold $\gamma_{th} = 0$. The figure shows that with the increase in the number of sources, the system can achieve a better outage performance. Also the decrease in the number of detected shares affect the performance significantly. The figure also compares the performance of the proposed scheme to the widely adopted An scheme [72], which shares the same underlying assumption of the non-availability of the CSI of the eavesdropper. It's noticeable that the proposed scheme outperform the AN scheme, even with less number of resources.

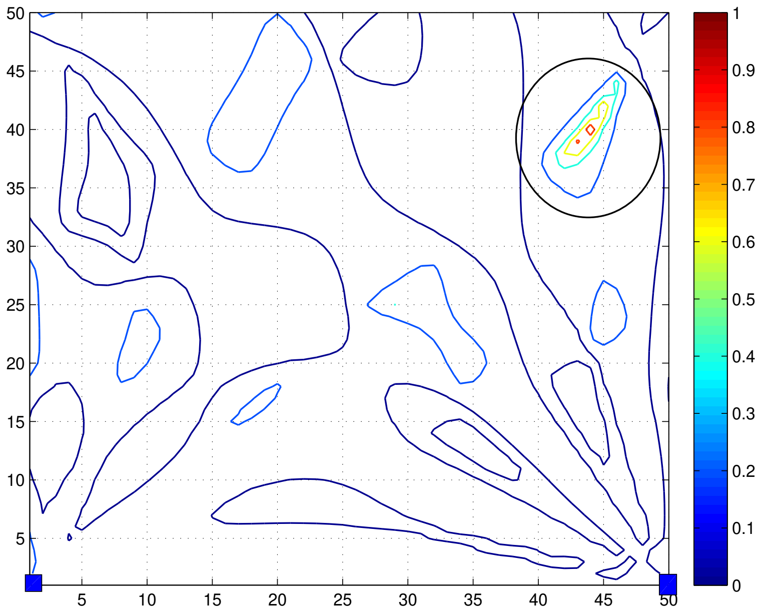


Figure 3.25: Signal correlation using two transmitters (case 2). The magnitude of correlation coefficient for the data of one of the users at the location (44,40) [inside the black circle]. The secret is shared using two sources [the blue squares].

3.3 Beam-Based NOMA

Secrecy was one aspect that directional transmission can enhance, another important aspect is system capacity. Directional transmission can help elevating the system capacity too. Here we provide our views on applying the NOMA scheme into directional transmission. Using NOMA helps achieving a grant free system, and possibly asynchronous transmission. Directionality here can help reducing the complexity of the multi-user processing. In this section, we will propose a strategy to integrate the NOMA approach with directional transmission.

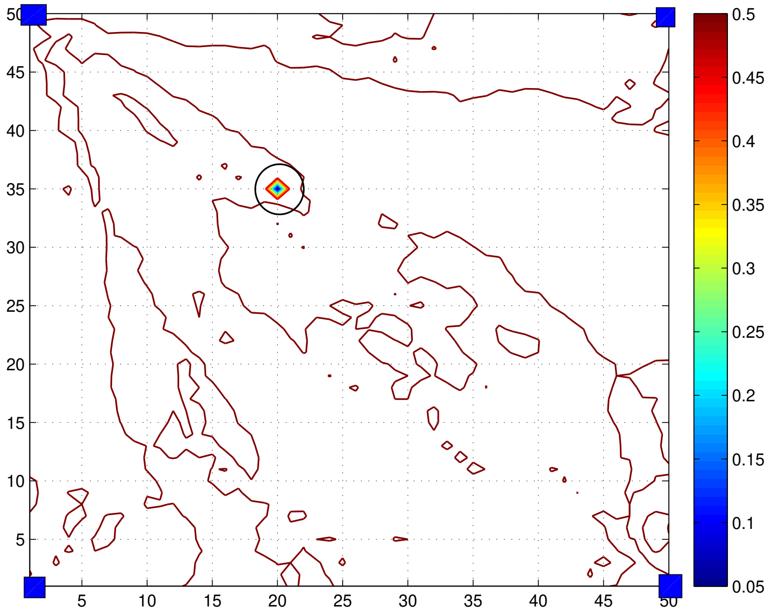


Figure 3.26: BER using four transmitters (case 1). BER for the data of one of the users at the location (20,35) [inside the black circle]. The secret is shared using four sources [the blue squares].

3.3.1 Signal Multiplexing

The base-station here is equipped with a uniform linear array (ULA)[8] of size N, with element spacing of $d = \lambda/2$, where λ is the carrier wavelength. In beam-space channel model, the angular domain is divided into N orthogonal basis each representing a physical angle ϕ_n [18]. Then, the corresponding channel response is given as,

$$\mathbf{G} = \mathbf{H}\mathbf{A}^{\dagger}, \tag{3.59}$$

[8] The assumption of ULA is made in order to simplify the analysis. The extension to multi-dimensional arrays is a straight-forward process with the use of the appropriate array response.

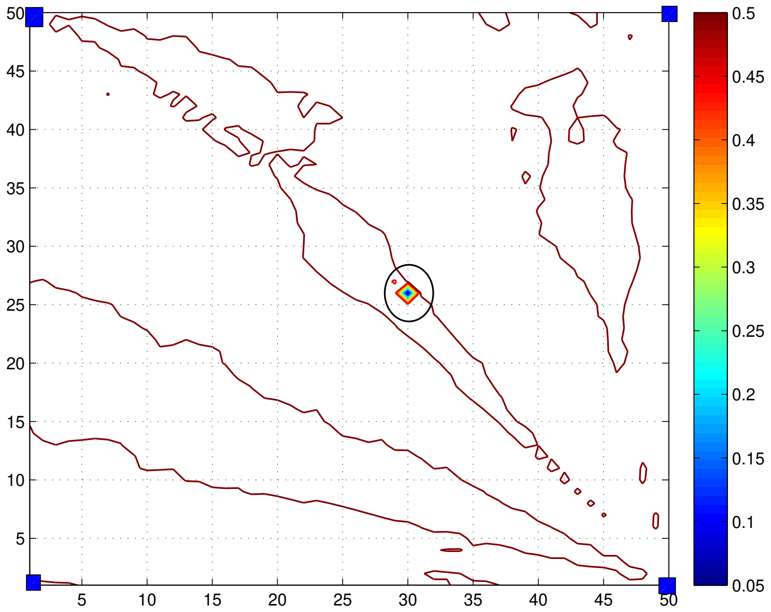


Figure 3.27: BER using four transmitters (case 2). BER for the data of one of the users at the location (30,26) [inside the black circle]. The secret is shared using four sources [the blue squares].

where $\mathbf{H} = \{h_{k,n}\}_{K\times N}$ is the i.i.d complex gain matrix, and $h_{k,n}$ represents the multi-path effect between the k^{th} user and the n^{th} transmission angle [73], K is the total number of users, and $\mathbf{A}$ is a unitary matrix which contains the array response of each of the orthogonal basis, and can be represented as,

$$\mathbf{A} = [\mathbf{a}(\theta_1), \mathbf{a}(\theta_2), \ldots, \mathbf{a}(\theta_N)], \tag{3.60}$$

where $\theta_n = \frac{\lambda}{Nd}\left(n - 1 - \frac{N-1}{2}\right)$ and $\phi_n = \arcsin(\theta_n)$. $a(\theta)$ represents the array response vector and can be given by,

$$\mathbf{a}(\theta) = \frac{1}{\sqrt{N}}\left[1, e^{-j\frac{2\pi d}{\lambda}\theta}, \ldots, e^{-j(N-1)\frac{2\pi d}{\lambda}\theta}\right]^T, \tag{3.61}$$

Based on this we can transmit N independent data streams towards these different angles, with the transmitted streams $\mathbf{t} = \{t_n\}_{N\times 1}$ given as:

$$\mathbf{t} = \mathbf{A}\mathbf{x}, \tag{3.62}$$

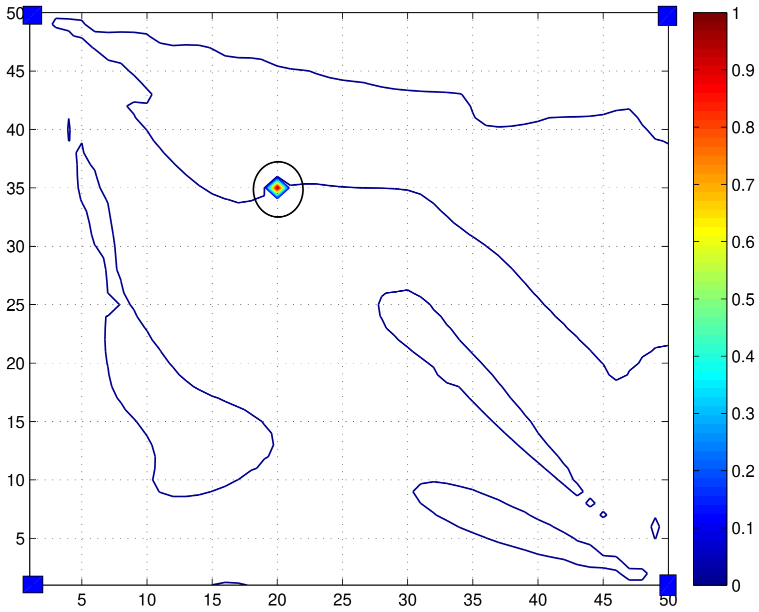


Figure 3.28: Signal correlation using four transmitters (case 1). The magnitude of correlation coefficient for the data of one of the users at the location (20,35) [inside the black circle]. The secret is shared using four sources [the blue squares].

where $\mathbf{x} = \{x_n\}_{N\times 1}$ is the vector containing the N independent streams. $\mathbf{A}$ is the precoding matrix which directs each stream towards the associated transmission angles. This resembles the discrete-Fourier-transform (DFT) process in OFDM system where each data stream is loaded on the corresponding sub-carrier.

Defining $\mathscr{M}_n$ which is the set of all users connected to the base-station through the n^{th} beam. Also, we define $\mathscr{J}_k$ which is the set of all beams connecting the k^{th} user to the base-station[9]. Then the data streams are constructed as,

$$x_n = \sum_{k\in\mathscr{M}_n} \sqrt{\beta_{k,n}P_n}\, s_k, \tag{3.63}$$

[9] We assume that $\mathscr{M}_n$ and $\mathscr{J}_k$ are known to the base-station through the channel estimation processes, and they are updated every time the estimation is done. This is applicable as the angle-of-arrival for the signal of each user is reciprocal to the angle-of-departure.

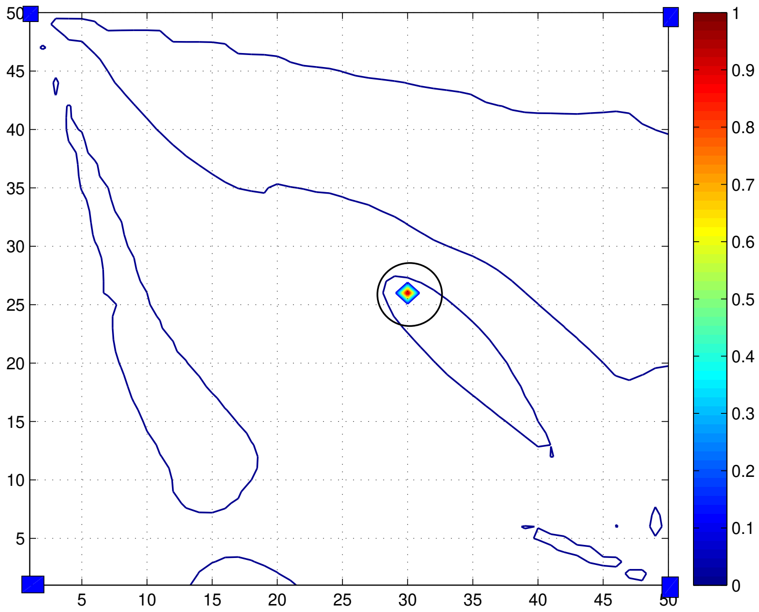


Figure 3.29: Signal correlation using four transmitters (case 2). The magnitude of correlation coefficient for the data of one of the users at the location (30,26) [inside the black circle]. The secret is shared using four sources [the blue squares].

where $\beta_{k,n}$ is the power fraction assigned to the k^{th} user in the n^{th} beam, and s_k is baseband modulated data. Equation (7) represents the superposition process of NOMA towards the n^{th} transmission direction.

The received signal at the k^{th} user is then given by,

$$r_k = \mathbf{g}_k \mathbf{t} + w_k = \sum_{n \in \mathscr{J}_k} g_n t_n + w_k, \tag{3.64}$$

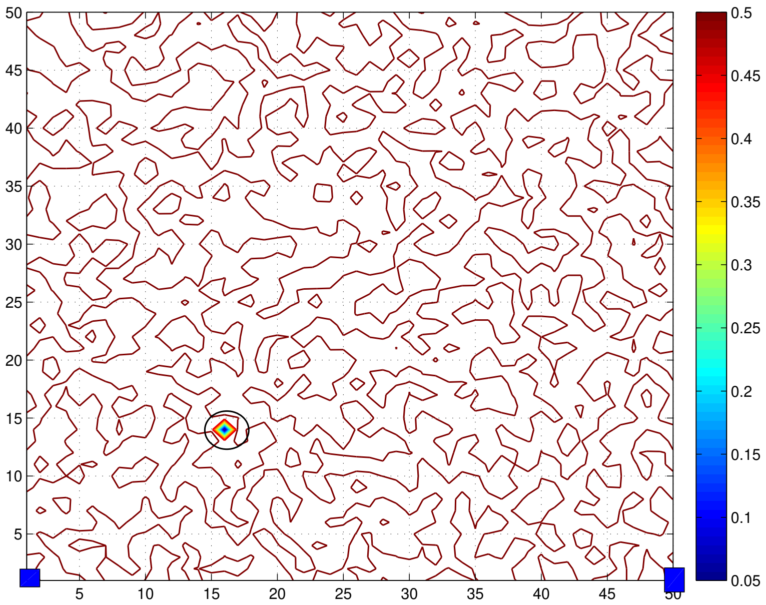


Figure 3.30: Effect of channel knowledge on secret sharing approach. BER for the data of one of the users at the location (16,14) [inside the black circle]. The secret is shared using two sources [the blue squares].

where $\mathbf{g}_k$ is the k^{th} row of $\mathbf{G}$ representing the channel vector of the k^{th} user, and w_k is an additive white Gaussian noise with zero mean and variance of σ_k^2. The unitary nature of $\mathbf{A}$ results in $\mathbf{Gt} = \mathbf{Hx}$. Then,

$$\begin{aligned} r_k =& \mathbf{h}_k \mathbf{x} + w_k = \sum_{n \in \mathscr{J}_k} h_{k,n} x_n + w_k, \\ =& \sum_{n \in \mathscr{J}_k} h_{k,n} \sqrt{\beta_{k,n} P_n}\, s_k \\ &+ \sum_{n \in \mathscr{J}_k} h_{k,n} \sum_{\substack{m \in \mathscr{M}_n \\ m \neq k}} \sqrt{\beta_{m,n} P_n}\, s_m + w_k. \end{aligned} \tag{3.65}$$

The first term of (3.65) represents the sum of all signals belongs to the k^{th} user from all $\mathscr{J}_k$ transmission directions. the second term represents the interference of the superimposed signals from the other $K-1$ users.

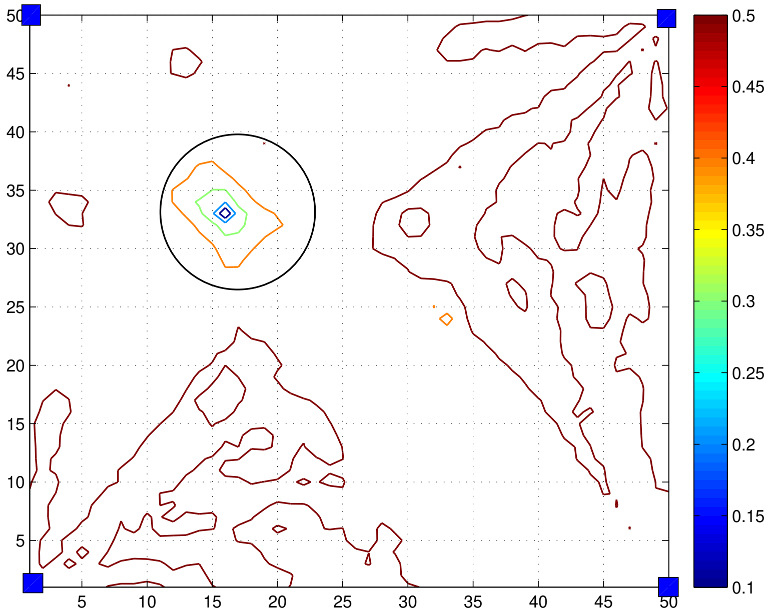


Figure 3.31: BER performance for single user case with secrecy sharing. BER for the data of one of the users at the location (16,33) [inside the black circle]. The secret is shared using two sources [the blue squares].

As a result, the received SINR γ_k, at the users with weak channel conditions, will be,

$$\gamma_k = \frac{\sum_{n \in \mathscr{I}_k} \left| h_{k,n} \sqrt{\beta_{k,n} P_n} \right|^2}{\sum_{n \in \mathscr{I}_k} \left| h_{k,n} \sum_{\substack{m \in \mathscr{M}_n \\ m \neq k}} \sqrt{\beta_{m,n} P_n} \right|^2 + \sigma_k^2}, \tag{3.66}$$

then the achievable rate is given by.

$$R_k = \log_2(1 + \gamma_k), \tag{3.67}$$

Here, we assume that users with higher quality channels are capable of applying perfect SIC, this lead to an enhanced effective SINR for these users in the form of,

$$\gamma_k^* = \frac{\sum_{n \in \mathscr{I}_k} \left| h_{k,n} \sqrt{\beta_{k,n} P_n} \right|^2}{\sigma_k^2}, \tag{3.68}$$

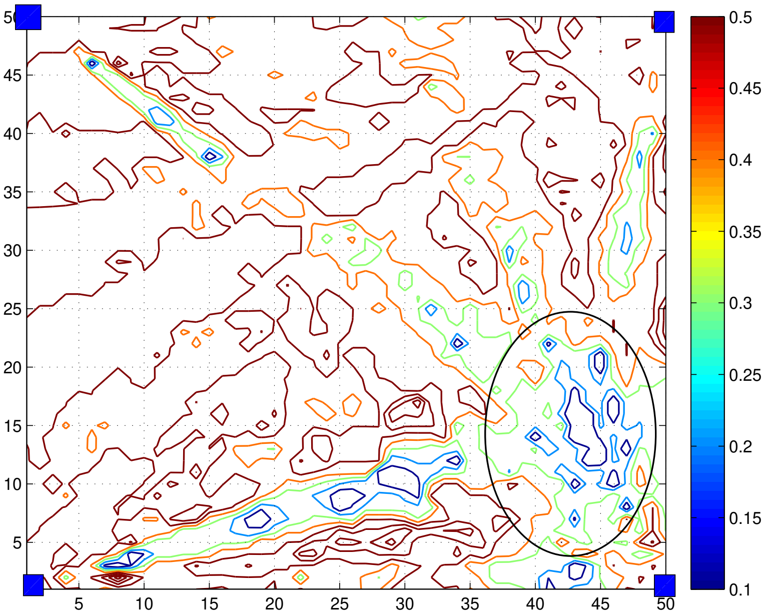


Figure 3.32: BER performance for single user case without secrecy sharing. BER for the data of one of the users at the location (44,15) [inside the black circle]. The secret is shared using four sources [the blue squares].

then, the achievable sum rate is given by,

$$R = \sum_{k=1}^{K} R_k. \tag{3.69}$$

Theorem 2. *The received SINR at any user before applying SIC follows the generalized beta prime distribution, $\beta^{'}(a,b,1,c)$, where,*

$$\begin{aligned} a &= |\mathscr{J}_k|_0 = N\delta \\ b &= N\delta \frac{\left(\sum_{\substack{m\in\mathscr{M}_n \\ m\neq k}} \beta_{m,n} + \frac{\sigma_k^2}{N\delta P_n}\right)^2}{\left(\sum_{\substack{m\in\mathscr{M}_n \\ m\neq k}} \beta_{m,n}\right)^2} \\ c &= \beta_{k,n} \frac{\left(\sum_{\substack{m\in\mathscr{M}_n \\ m\neq k}} \beta_{m,n} + \frac{\sigma_k^2}{N\delta P_n}\right)}{\left(\sum_{\substack{m\in\mathscr{M}_n \\ m\neq k}} \beta_{m,n}\right)^2} \end{aligned} \tag{3.70}$$

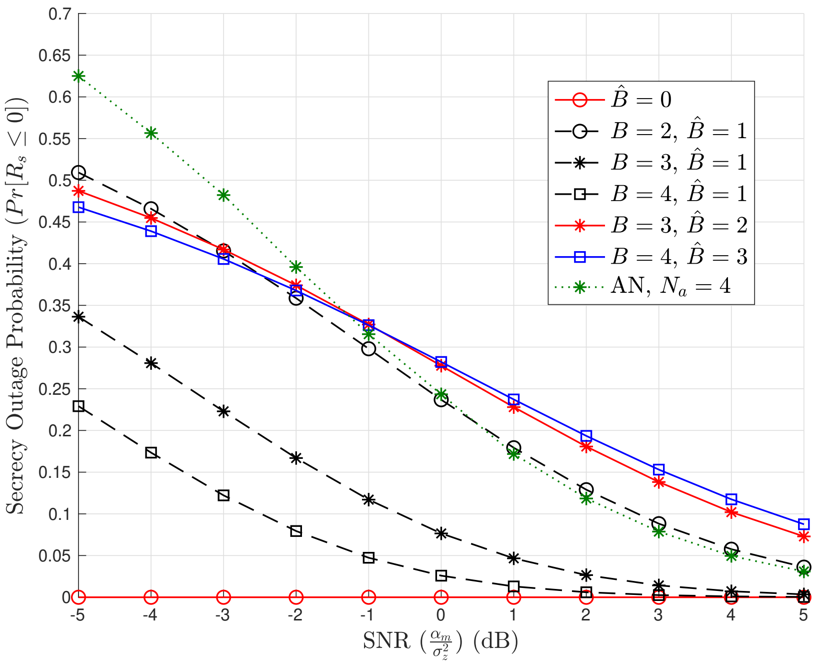


Figure 3.33: Outage probability with secret-sharing. Secrecy outage probability of the system for different number of sources B, and different number of collected shares $\hat{B}$, with secrecy threshold $\gamma_{th} = 0$.

Proof. This is a straightforward process. The channel coefficients h_n are considered as i.i.d. complex Gaussian random variables ($h_n \sim \mathcal{N}(0,1)$), hence,

$$\sum_{n \in \mathcal{J}_k} \beta_{k,n} P_n |h_{k,n}|^2 \sim \Gamma\left(|\mathcal{J}_k|_0, P_n \beta_{k,n}\right), \tag{3.71}$$

similarly,

$$\sum_{n \in \mathcal{J}_k} P_n \left| h_{k,n} \sum_{\substack{m \in \mathcal{M}_n \\ m \neq k}} \sqrt{\beta_{m,n}} \right|^2 \sim \Gamma\left(|\mathcal{J}_k|_0, P_n \sum_{\substack{m \in \mathcal{M}_n \\ m \neq k}} \beta_{m,n} \right), \tag{3.72}$$

The denominator in (3.66) shifts the mean of (3.72) with the value σ_k^2, this changes the distribution in (3.72) to $\Gamma(b, \frac{P_n \beta_{k,n}}{c})$. The ratio of these Gamma random variables follows the generalized beta prime distribution. □

Corollary 1. *The effective SNR after applying SIC follows the Gamma distribution,* $\Gamma\left(|\mathscr{J}_k|_0, \frac{P_n\beta_{k,n}}{\sigma_k^2}\right)$.

3.3.2 Power Allocation

Power allocation is one of the most critical parts of any NOMA scheme. Our target here is to maximize the achievable sum rate, keeping in mind that there is a maximum power constraint of P_n per beam , this can be formulated as follows,

$$\begin{aligned} \underset{\beta}{\text{maximize}} \quad & R_n \\ \text{subject to} \quad & \sum_{k\in\mathscr{M}_n} \beta_{k,n} \leq 1. \end{aligned} \tag{3.73}$$

Sum rate maximization problem is known to be a non-convex problem [74]. Moreover, here we need to solve two joint issues, the distribution of power between different users, and the distribution of power between different beams for each of the users.

In order to simplify the problem, we adopt the Max-Min SINR approximation of the problem in (3.73), which is given as,

$$\begin{aligned} \underset{\beta}{\text{maximize}} \quad & \underset{k}{\min} \quad \gamma_k \\ \text{subject to} \quad & ||\beta|| \leq \sqrt{N}. \end{aligned} \tag{3.74}$$

this problem can be solved using Algorithm 2 [75]. A further simplification can be done by solving each of these issues separately. In such context, the power factor can be rewritten as $\beta_{k,n} = \varepsilon_n^k \rho_k$, where ρ_k represents the portion of power given to the k^{th} user, and ε_n^k is the amount of ρ_k directed towards the n^{th} beam.

Regarding the distribution of the power over the beams for each user, we adopt a water-filling approach [76][10]. So the beam power distribution is given as,

$$\varepsilon_n^k = \left[\frac{1}{\mathscr{L} - \frac{\sigma_k^2}{|h_{k,n}|^2}}\right]^+ \qquad \forall n \in \mathscr{J}_k \tag{3.75}$$

where $\mathscr{L}$ is the Lagrange multiplier chosen to ensure the power constraint $\sum_{n \in \mathscr{J}_k} \varepsilon_n^k = 1$.

Afterwards, $\mathbf{p} = [\rho_1, \rho_2, \ldots, \rho_K]$ is found as,

$$\begin{aligned} &\underset{\mathbf{p}}{\text{maximize}} \quad \min_{k} \quad \gamma_k \\ &\text{subject to} \quad |\mathbf{p}| \leq 1, \end{aligned} \tag{3.76}$$

similarly, this can be solved using Algorithm 2.

Another aspect, which a concern in this scheme, is the number of active beams per user $|\mathscr{J}_k|_0$. More precisely, the ratio between the active beams and and the total number of beams which we note as the activation ratio $(0 < \delta \leq 1)$. With the value of δ approaches unity, this means that each user almost has interference from all other users in the system, which will degrade the performance of the system.

Algorithm 2 Max-Min SINR

```
Update power $\mathbf{p}(l+1)$:
    $\rho_k(l+1) \leftarrow \frac{\rho_k(l+1)}{\gamma_k(\mathbf{p}(l))} \quad \forall k$
Normalize $\mathbf{p}(l+1)$:
    $\rho_k(l+1) \leftarrow \frac{\rho_k(l+1)}{\max_i \rho_i(l+1)} \quad \forall k$
```

On the other hand, if the value of δ moves towards zero, this means that the interference will be limited, but the system may not be able to provide enough diversity to all users in the system. Limited diversity may favor some users compared to others, which may cause a poor fairness performance.

[10] This step represents the case where the k^{th} user is assigned p_k power fraction of the total power, hence, how would that fraction be distributed over the different beams serving the k^{th} user.

Another approach for optimizing the power allocation could be based on weighted sum rate,

$$\begin{aligned} \underset{\beta}{\text{maximize}} \quad & \frac{1}{N}\sum_{k=1}^{K} \mu_k R_k \\ \text{subject to} \quad & \sum_{k\in\mathscr{M}_n} \beta_{k,n} \leq 1. \end{aligned} \tag{3.77}$$

where μ_k is a predefined priority factor of the k^{th} user. This approach could achieve a better fairness between users. The predefined priority factors μ can be calculated based on either the quality of service (QoS) requirements of each user, or the average rate achieved by a user over a certain amount of time.

3.3.3 Performance

In order to be able to compare to the MIMO-NOMA and MIMO-OMA, we assume the total number of users K is twice the number of the available beams (i.e., $K = 2N$). The MIMO-OMA users are assumed to share the resources equally, so each of them is only allowed half of the spatial resources. The achievable sum rate of the K users then is normalized to the total number of available beams. The cell is serving $2N$ users which are randomly distributed over the area covered by that cell. The distribution of the users in the cell follows a Poisson point process as adopted by cellular systems.

Figure 3.34 shows the average sum rate per channel use against the average SNR (i.e., transmit SNR $\frac{N\delta P_n}{\sigma^2}$). As previously mentioned the activation ratio δ highly affect the performance of the system. From the figure, we can see that the increase of that ratio reduces the gain of the system compared to NOMA, which is expected as the number of interfering users per beam is increasing. On the other side, low values of δ allow the system to achieve higher rates.

Furthermore, figure 3.34 shows that the adoption of the joint power optimization approach would yield a better overall performance for the proposed system. the enhanced performance for the lower δ values suggested that the system is more suitable for sparse channel, which is an adopted feature for mm-wave environments.

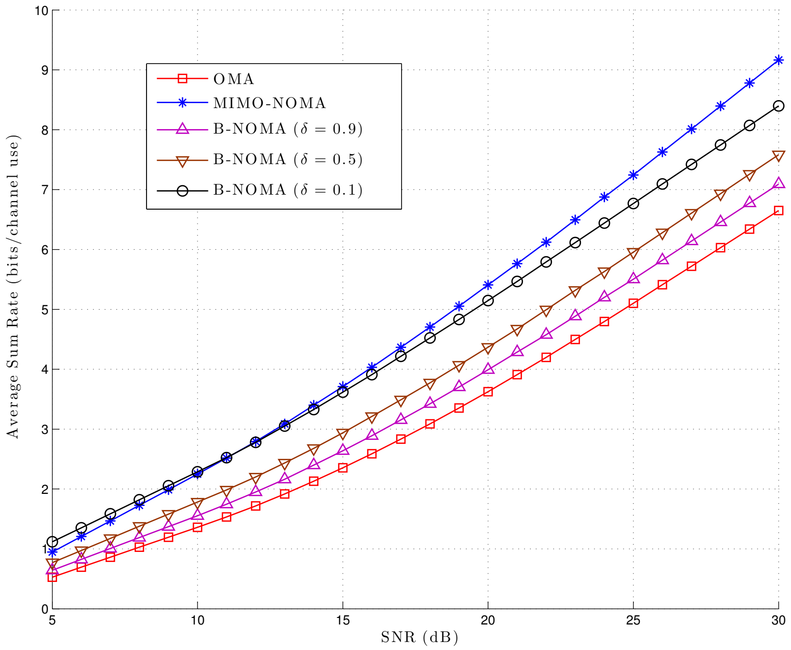


Figure 3.34: Average sum rate. The figure compares the Sum rate to the current state of the art.

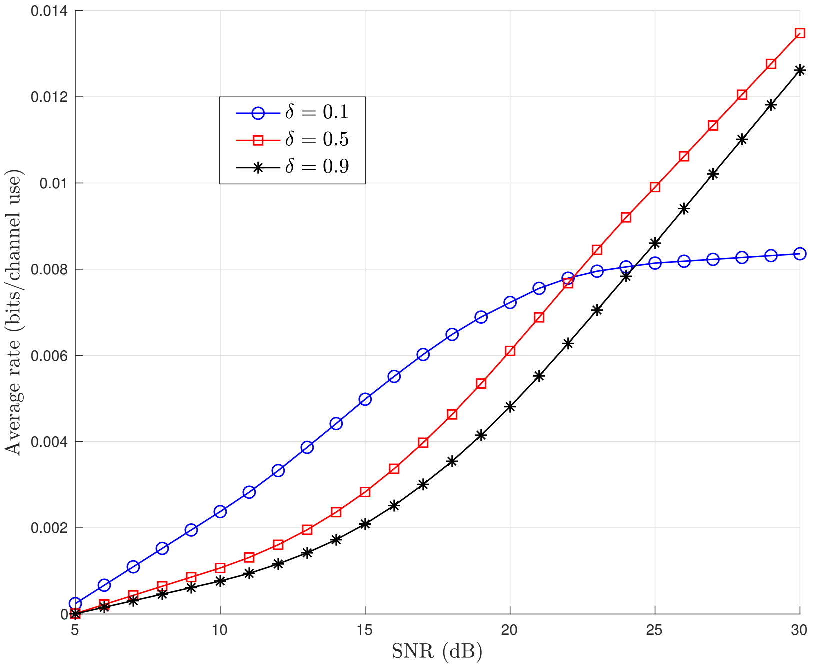


Figure 3.35: Weak link average rate. The figure shows the change of the weak link rate.

Figure 3.35 shows the effect of the activation ratio on the weak users of the system. Even though, the lower activation ratio provide a better overall performance for the system, the achievable rate for the weak users is limited, which as explained before may be the result of low diversity order. On the other hand, a higher activation ratio allow weak users to achieve better rates, but on the expense of lower overall performance.

On the other hand, figure 3.36 shows the effect of the activation ratio on user with the best link condition in the system. Unlike the user with the weakest link condition, increasing the activation ratio reduce the achievable rate. This is due the effect of the increased interference in the system, which reduces the overall performance. Also, by allowing more diversity, The power is distributed over more links, which reduces the overall portion of power given to that user.

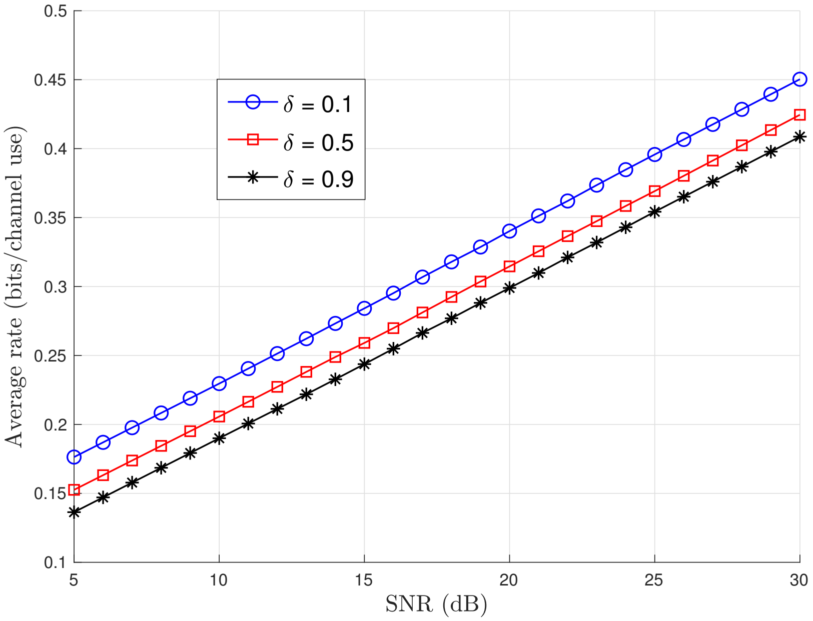


Figure 3.36: Strong link average rate. The figure shows the change of the strong link rate.

Figure 3.37 shows how the beam activation ratio affect the average rates of the strongest and weakest links of the system. Different users have different optimum values for δ, which make an application-based optimization for the activation ratio is necessary[11]. On another side, mm-wave channels have a sparse structure, which will keep the system operational at lower values of δ by default.

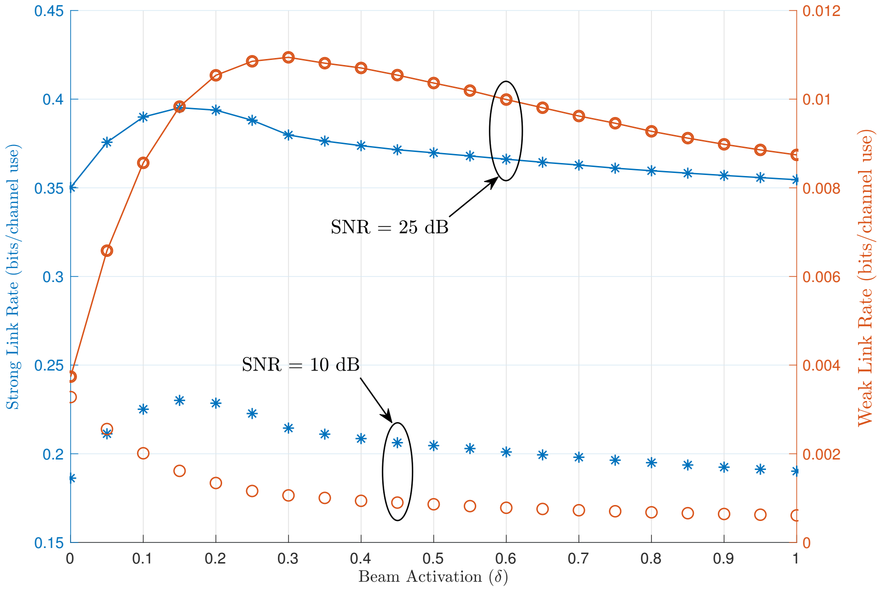


Figure 3.37: Activation ratio effect. The figure shows the effect of activation ratio on the rate of different links.

[11] the optimization of the activation ratio, and the associated active beams assignments are considered as a future extension for this work.

Chapter 4: Industrial Experience:
3GPP-NR Uplink Physical Control Channels and Signals

During Summer/Fall 2018, I was blessed to have the opportunity to work at Intel corporation as an Intern. I worked under the next generation and standards group, to develop and test physical layer algorithms for 5G-NR based communications units. This chapter briefly discuss the main concepts I worked on during my Internship.

Table 4.1: Structure of 5G-NR PUCCH formats

Structure of PUCCH Formats			
Format	# OFDM symbols	# Physical Resource Blocks	# Bits
0	$1 \rightarrow 2$	1	$\leq 2+SR$
1	$4 \rightarrow 14$	1	≤ 2
2	$1 \rightarrow 2$	$1 \rightarrow 16$	> 2
$3/4$	$4 \rightarrow 14$	$1 \rightarrow 16$	> 2

4.1 Physical Uplink Control Channel (PUCCH)

Uplink control channel is used to provide three main information data from the UE to the base-station, namely, hybrid automatic repeat request (HARQ), scheduling request (SR), and channel state information(CSI). Furthermore, CQI carries some indicators, namely, rank indicator (RI), precoding matrix indicator (PMI), channel quality indicator (CQI). In order to feedback these information to the gNB, NR provides 5 different formats that can be used by the UE, as shown in Table 4.1 [77]. The available formats, there structure, and uses are described in the following sections.

4.1.1 Format 0

Format 0 adopts a sequence based transmission scheme. This format is a short duration format, which spans only up to 2 OFDM symbols. It can be used to transmit 1 or 2 HARQ bits, in addition to a SR flag. The occupied symbols are allocated starting from the end of the slot, and spans a single physical resource block (PRB).

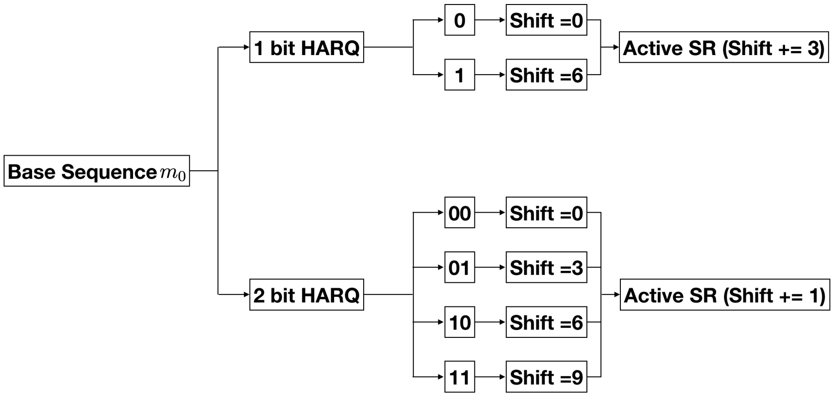


Figure 4.1: Format 0 bit mapping.

A length 12 low PAPR base sequence is used to transmit the HARQ and SR information. Each combination of bits is given a different cyclic shift of that base sequence, as shown in figure 4.1 [78]. With active SR an additional shift is presented to the sequence.Even though, the demodulation reference signals(DMRS) based approach shows better performance for low delay spread channels,the sequence based approach reduce the overhead imposed in case of using DMRS. Also, it avoids the error propagation caused from the channel estimation errors. Moreover, the performance of the sequence based approach is superior in long delay spread channels [79].

In order for the receiver to retrieve this information, an algorithm is required to detect the corresponding cyclic shift. The performance of the HARQ processes is measured using ACK error rate (i.e., missed ACKs and ACK-to-NACK errors), False alarm rate (i.e., DTX-to-ACK errors), and NACK-to-ACK error rate. A correlation-based receiver can be used to detect the cyclic shift as follows,

$$m_{cs} = \arg\max_{m} \quad c(m) = \frac{|r \cdot s_m^*|}{||r||^2} \geq c_{th}, \tag{4.1}$$

where r is the received sequence, s_m is the base sequence with a cyclic shift equal to m, and $m = \{0, 1, \ldots, 11\}$. The false alarm threshold $c_{th} = f(n, P_{fa})$ is a function of the diversity order n and false alarm probability P_{fa}. The standard contributions suggest the false alarm rate to be set to 10^-2. The threshold c_{th} is an inverse incomplete-gamma-function, which doesn't have a closed-form but can be approximated.

4.1.2 Format 2

Another short duration format is format 2. Similar to format 0 it can occupy up to 2 OFDM symbols with frequency hopping optional, but it can span up to 16 PRB. Format 2 has a DMRS-based structure as shown in figure 4.2, with DMRS symbols inserted every third subcarrier. UCI bits are channel coded before being modulated to QPSK symbols. This format support the transmission of UCI bit load larger than 2 bits.

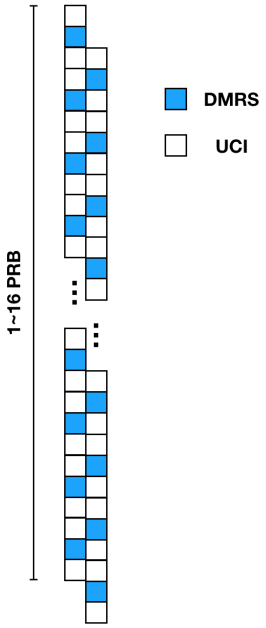


Figure 4.2: Grid structure of format 2.

As the structure spans a very short duration in time (1 or 2 symbols), High values of frequency offset/Doppler shift will not leave a significant effect on the performance. on the other hand, the occupied frequency is relatively large, which makes the performance considerably affected in case of the existence of large time-offset values.The $1/3$ (DMRS/UCI) ratio provide decent amount of resources to perform parameters estimation processes.

Time-offset needs to be estimated and corrected before the channel estimation step. a simple DMRS sample correlation approach can provide a reliable estimate for time-offset. Another parameter that is required before channel estimation is the SNR. SNR can be estimated using a simple moments-based estimator [80]. After eliminating the the time-offset rotation, the SNR can be used to generate a channel estimate for UCI samples, which in turn will be used to demodulate these samples.

4.1.3 Format 1

Format 1 is a long duration format spanning 4 to 14 OFDM symbols. It supports the transmission of up to 2 UCI bits, and it occupies a single PRB. DMRS samples are distributed to occupy the whole frequency band every other OFDM symbol, as shown in figure 4.3. This high density of DMRS samples provides very high reliability for parameters estimation. Moreover, the high repetition rate of the UCI bits provides a high coding gain. The UCI are directly modulated to either BPSK or QPSK symbols. Format 1 also supports multi-user multiplexing over the same resources using OCC spreading codes.

As format 1 structure span only a single PRB, only high time-offset values would affect its performance. Therefore a precise time-offset estimation is not needed, only a hypotheses testing for a limited number of values could be sufficient (e.g., $\{0, 0.25, 0.5\}$ CP length). With the frequent DMRS time allocation, a reliable frequency-offset estimation and correction can be implemented. Then, the channel can be estimated over the DMRS symbols, and interpolated over UCI data symbols. The high density of DMRS symbols can provide a reliable SNR estimate to assist channel estimation.

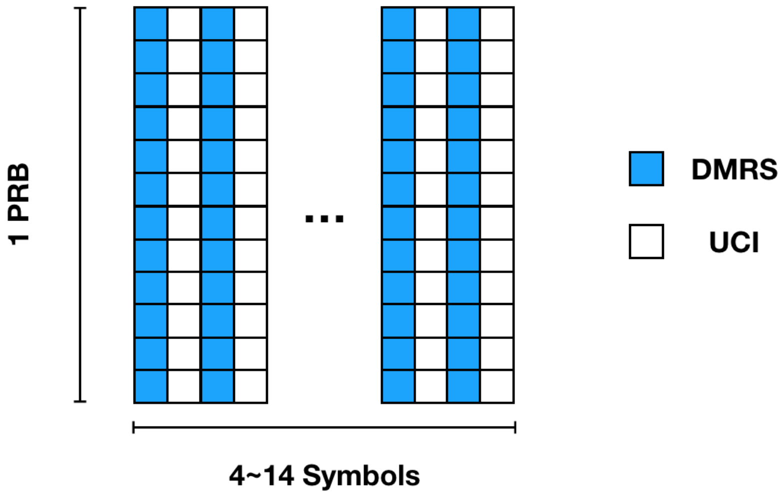


Figure 4.3: Grid structure of format 1.

4.1.4 Formats 3/4

The other long duration formats are 3/4. both formats share the same grid structure, but format 4 support multi-user multiplexing, while format 3 doe snot support that option. These formats are used to transmit UCI data of a size larger than 2 bits. Similar to format 1, they can occupy up to 14 OFDM symbols and span up to 16 PRB. DMRS symbols are inserted in the middle of each slot, with the option of having additional DMRS symbols. Figure 4.4 shows an example for the DMRS placement in case of 10 OFDM symbols, for both options.

With the high density of the DMRS in the frequency domain, a reliable time-offset and SNR estimates can be obtained. A frequency-offset would be possible to obtain in certain cases, but not always. To get a frequency offset estimate, either the additional DMRS option should be active, or the frequency hopping should not be active. So, these formats are not suggested for high mobility applications.

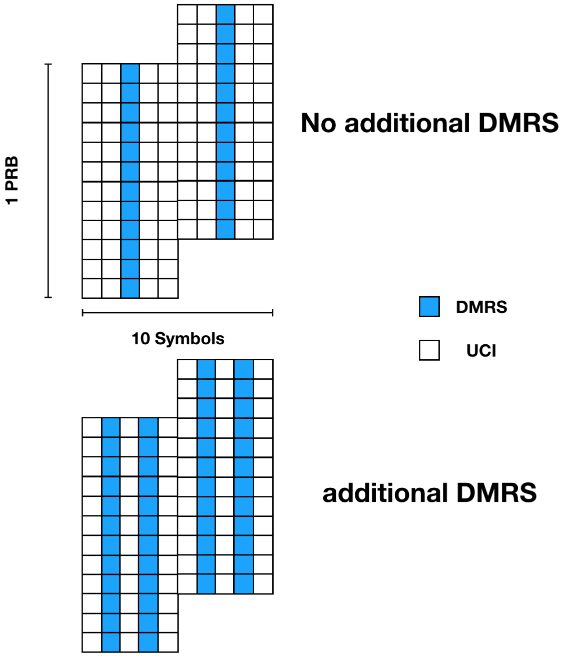


Figure 4.4: Grid structure example of formats 3/4.

4.2 Sounding Reference Signal (SRS)

SRS is sent from the UE to the gNB in order to provide means of uplink channel evaluation. Based on the channel quality induced from SRS at gNB, the gNB can decide on the scheduling information for each UE. These information include the RI, TPMI, and MCS. based on these information, the gNB assign a transmission band, modulation scheme, coding rate, and spatial precoding matrix. Also, it sends this information to the UE in the PDDCH, in order to be able to decode the data. In order to be able to link the channel quality to the relative parameter a calibration process is required in order to meet either a quality of service goal or an error rate target.

Figure 4.5 shows the grid structure of the SRS signals. SRS can occupy either 1, 2, and 4 OFDM symbols. These symbols can span between 4 and 272 PRBs. As shown in the figure,SRS has to modes of multiplexing, namely, ’Comb 2’ and ’Comb 4’. The Comb size defines the frequency spacing for each SRS signal, and in turn the number of SRS signals that can be multiplexed on the same symbol.

The received SRS signal can be used for parameter estimation (e.g., SNR, time-offset, frequency-offset, antenna correlation). These estimates can be used along with the SRS signal to estimate the channel. Then, using the estimated channel and the available set of precoding matrices to generate a dictionary for all possible effective channels. The effective channel that yields the best capacity is determined and the corresponding PMI and RI are selected. Then, based on the capacity value, the highest MSC value that can achieve the desired Qos requirement is selected.

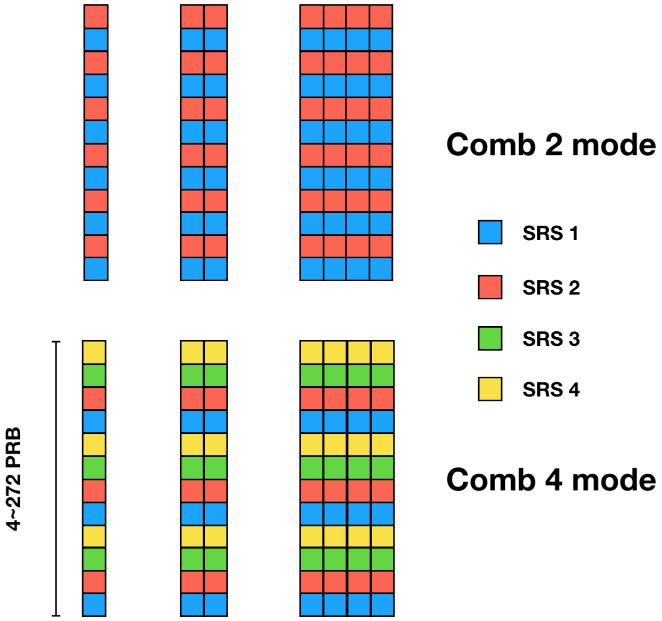


Figure 4.5: Grid structure of SRS.

Chapter 5: Concluding Remarks

In this dissertation, we provided an overview of the usage of directional transmission to enhance the quality of wireless communication systems, and provide secrecy through physical layer processing. A review for all the related topics was provided to ensure a solid background for the basics of this topic. We revised the basics of multiple- antenna systems and related channel models. Moreover, we reviewed the basics of physical layer security and how multiple antenna systems can contribute to providing secrecy. Also, we covered non-orthogonal multiple access, which is recently considered one of the enabling technologies for ultra-low-latency communications, and how multiple antenna systems can help to enhance its performance.

Based on the provided literature review, we proposed several approaches to enhance both secrecy and system capacity. First, we provided a new scheme for transmitting multiple data stream towards multiple directions, simultaneously, using the directional modulation approach. The scheme is capable of providing an independent and secure communication link for each transmission direction. Moreover, we were able to reduce the complexity of the transmission scheme using a DFT based synthesis module.

Using the multiple directions approach, we introduced a location-based secrecy system. This system can be utilized either in a single cell system or in a centralized/cloud radio access network (C-RAN). The system can provide a secure geographical region for each legitimate user in the network, through joint transmission processing between all transmission nodes. To further enhance the performance, we added multiple node cryptography that makes it highly unlikely for eavesdroppers to acquire any information.

For enhancing system capacity, we proposed a directional based NOMA scheme. The scheme is aimed to reduce the load imposed on the scheduler by the user pairing approach. Moreover, the scheme allows the pairing of more than two users over the same resource and can provide rates close to the state of the art systems. Finally, to grasp the experience acquired on the internship at Intel corporation, we provided an overview of the uplink physical channels and signals and the related design aspects.

References

[1] S. Lien, S. Shieh, Y. Huang, B. Su, Y. Hsu, and H. Wei, “5G new radio: Waveform, frame structure, multiple access, and initial access,” *IEEE Communications Magazine*, vol. 55, no. 6, pp. 64–71, June 2017.

[2] A. A. Zaidi, R. Baldemair, H. Tullberg, H. Bjorkegren, L. Sundstrom, J. Medbo, C. Kilinc, and I. Da Silva, “Waveform and numerology to support 5G services and requirements,” *IEEE Communications Magazine*, vol. 54, no. 11, pp. 90–98, November 2016.

[3] Z. E. Ankarali, B. Peköz, and H. Arslan, “Flexible radio access beyond 5G: A future projection on waveform, numerology, and frame design principles,” *IEEE Access*, vol. 5, pp. 18 295–18 309, 2017.

[4] N. Michailow, M. Matthé, I. S. Gaspar, A. N. Caldevilla, L. L. Mendes, A. Festag, and G. Fettweis, “Generalized frequency division multiplexing for 5th generation cellular networks,” *IEEE Transactions on Communications*, vol. 62, no. 9, pp. 3045–3061, Sep. 2014.

[5] B. Farhang-Boroujeny, “OFDM versus filter bank multicarrier,” *IEEE Signal Processing Magazine*, vol. 28, no. 3, pp. 92–112, May 2011.

[6] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, “Massive MIMO for next generation wireless systems,” *IEEE Communications Magazine*, vol. 52, no. 2, pp. 186–195, February 2014.

[7] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, “Millimeter wave mobile communications for 5G cellular: It will work!” *IEEE Access*, vol. 1, pp. 335–349, 2013.

[8] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 1617–1655, thirdquarter 2016.

[9] L. Dai, B. Wang, Y. Yuan, S. Han, C. I, and Z. Wang, "Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 74–81, September 2015.

[10] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of things in the 5G era: Enablers, architecture, and business models," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 510–527, March 2016.

[11] A. F. Demir, Z. E. Ankarali, Q. H. Abbasi, Y. Liu, K. Qaraqe, E. Serpedin, H. Arslan, and R. D. Gitlin, "In *vivo* communications: Steps toward the next generation of implantable devices," *IEEE Vehicular Technology Magazine*, vol. 11, no. 2, pp. 32–42, June 2016.

[12] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, April 2018.

[13] Lizhong Zheng and D. N. C. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels," *IEEE Transactions on Information Theory*, vol. 49, no. 5, pp. 1073–1096, May 2003.

[14] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 8, pp. 1451–1458, Oct 1998.

[15] A. Goldsmith, S. A. Jafar, N. Jindal, and S. Vishwanath, "Capacity limits of MIMO channels," *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 5, pp. 684–702, June 2003.

[16] A. S. Y. Poon, R. W. Brodersen, and D. N. C. Tse, “Degrees of freedom in multiple-antenna channels: a signal space approach,” *IEEE Transactions on Information Theory*, vol. 51, no. 2, pp. 523–536, Feb 2005.

[17] F. Darbari, R. W. Stewart, and I. A. Glover, “Mimo channel modelling,” in *Signal Processing*, S. Miron, Ed. Rijeka: IntechOpen, 2010, ch. 5.

[18] A. M. Sayeed, “Deconstructing multiantenna fading channels,” *IEEE Transactions on Signal Processing*, vol. 50, no. 10, pp. 2563–2579, Oct 2002.

[19] L. S. X. Zhou and Y. Zhang, *Physical layer security in wireless communications*. Boca Raton, FL: CRC Press, 2013.

[20] C. Shannon, “Communication theory of secrecy systems,” *Bell Syst. Tech. J.*, vol. 29, pp. 656–715, 1949.

[21] A. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[22] Z. Jia-jie, P. Jian-hua, H. Kai-zhi, and J. Jiang, “A multi-user MIMO system encryption algorithm based on joint channel state matrix,” in *Proceedings of 2011 International Conference on Computer Science and Network Technology*, vol. 3, Dec 2011, pp. 1452–1455.

[23] A. Mukherjee and A. L. Swindlehurst, “Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels,” in *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sept 2009, pp. 1134–1141.

[24] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third 2014.

[25] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, “Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper,” *IEEE Transactions on Vehicular Technology*, vol. 63, no. 4, pp. 1678–1690, May 2014.

[26] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, “Secrecy outage in MISO systems with partial channel information,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 704–716, April 2012.

[27] M. Yuksel and E. Erkip, “Diversity-multiplexing tradeoff for the multiple-antenna wire-tap channel,” *IEEE Transactions on Wireless Communications*, vol. 10, no. 3, pp. 762–771, March 2011.

[28] N. Wang, N. Zhang, and T. A. Gulliver, “Cooperative key agreement for wireless networking: Key rates and practical protocol design,” *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 272–284, Feb 2014.

[29] J. M. Hamamreh, H. M. Furqan, and H. Arslan, “Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey,” *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2019.

[30] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas part I: The MISOME wiretap channel,” *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[31] S. A. A. Fakoorian and A. L. Swindlehurst, “Optimal power allocation for GSVD-based beamforming in the MIMO gaussian wiretap channel,” in *2012 IEEE International Symposium on Information Theory Proceedings*, July 2012, pp. 2321–2325.

[32] X. Zhang, X. Zhou, and M. R. McKay, “On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels,” *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2170–2181, Jun 2013.

[33] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, “Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding,” *IEEE Transactions on Communications*, vol. 60, no. 11, pp. 3472–3482, November 2012.

[34] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin, “Securing massive MIMO at the physical layer,” in *2015 IEEE Conference on Communications and Network Security (CNS)*, Sep. 2015, pp. 272–280.

[35] E. Tekin and A. Yener, “The gaussian multiple access wire-tap channel,” *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5747–5755, Dec 2008.

[36] Y. Saito, A. Benjebbour, Y. Kishiyama, and T. Nakamura, “System-level performance evaluation of downlink non-orthogonal multiple access (NOMA),” in *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Sept 2013, pp. 611–615.

[37] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, “A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends,” *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2181–2195, Oct 2017.

[38] N. H. Mahmood, M. Lauridsen, G. Berardinelli, D. Catania, and P. Mogensen, “Radio resource management techniques for eMBB and mMTC services in 5G dense small cell scenarios,” in *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, Sept 2016, pp. 1–5.

[39] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, C. I, and H. V. Poor, “Application of non-orthogonal multiple access in lte and 5G networks,” *IEEE Communications Magazine*, vol. 55, no. 2, pp. 185–191, February 2017.

[40] T. Wirth, M. Mehlhose, J. Pilz, B. Holfeld, and D. Wieruch, “5G new radio and ultra low latency applications: A PHY implementation perspective,” in *2016 50th Asilomar Conference on Signals, Systems and Computers*, Nov 2016, pp. 1409–1413.

[41] S. Chen, B. Ren, Q. Gao, S. Kang, S. Sun, and K. Niu, “Pattern division multiple access: A novel nonorthogonal multiple access for fifth-generation radio networks,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3185–3196, April 2017.

[42] Q. H. Spencer, A. L. Swindlehurst, and M. Haardt, “Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels,” *IEEE Transactions on Signal Processing*, vol. 52, no. 2, pp. 461–471, Feb 2004.

[43] S. M. R. Islam, N. Avazov, O. A. Dobre, and K. Kwak, “Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges,” *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 721–742, Secondquarter 2017.

[44] C. Yan, A. Harada, A. Benjebbour, Y. Lan, A. Li, and H. Jiang, “Receiver design for downlink non-orthogonal multiple access (NOMA),” in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, May 2015, pp. 1–6.

[45] M. Zeng, A. Yadav, O. A. Dobre, G. I. Tsiropoulos, and H. V. Poor, “On the sum rate of MIMO-NOMA and MIMO-OMA systems,” *IEEE Wireless Communications Letters*, vol. 6, no. 4, pp. 534–537, Aug 2017.

[46] S. M. R. Islam, M. Zeng, O. A. Dobre, and K. Kwak, “Resource allocation for downlink NOMA systems: Key techniques and open issues,” *IEEE Wireless Communications*, vol. 25, no. 2, pp. 40–47, April 2018.

[47] Z. Yuan, G. Yu, W. Li, Y. Yuan, X. Wang, and J. Xu, “Multi-user shared access for internet of things,” in *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, May 2016, pp. 1–5.

[48] H. Nikopour and H. Baligh, “Sparse code multiple access,” in *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Sept 2013, pp. 332–336.

[49] Z. Zhao, D. Miao, Y. Zhang, J. Sun, H. Li, and K. Pedersen, “Uplink contention based transmission with non-orthogonal spreading,” in *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, Sept 2016, pp. 1–6.

[50] M. Hafez and H. Arslan, “On directional modulation: An analysis of transmission scheme with multiple directions,” in *2015 IEEE International Conference on Communication Workshop (ICCW)*, June 2015, pp. 459–463.

[51] M. Hafez, T. Khattab, T. Elfouly, and H. Arslan, “Secure multiple-users transmission using multi-path directional modulation,” in *2016 IEEE International Conference on Communications (ICC)*, May 2016, pp. 1–5.

[52] M. Hafez, M. Yusuf, T. Khattab, T. Elfouly, and H. Arslan, “Secure spatial multiple access using directional modulation,” *IEEE Transactions on Wireless Communications*, vol. 17, no. 1, pp. 563–573, Jan 2018.

[53] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York, NY, USA: Cambridge University Press, 2004.

[54] Y. Ding and V. F. Fusco, “Establishing metrics for assessing the performance of directional modulation systems,” *IEEE Transactions on Antennas and Propagation*, vol. 62, no. 5, pp. 2745–2755, May 2014.

[55] J. Skold, “Base station (BS) radio transmission and reception,” 3rd Generation Partnership Project (3GPP), Technical specification (TS) 36.104, Jul. 2018.

[56] P. S. Diniz, *Adaptive Filtering: Algorithms and Practical Implementation*, 2nd ed. Norwell, MA, USA: Kluwer Academic Publishers, 2002.

[57] M. Yusuf and H. Arslan, “Secure multi-user transmission using CoMP directional modulation,” in *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, Sept 2015, pp. 1–2.

[58] C. Oberli and M. Garcia, "Intercarrier interference in OFDM: A deterministic model for transmissions in mobile environments with imperfect synchronization," in *2008 IEEE International Symposium on Wireless Communication Systems*, Oct 2008, pp. 37–41.

[59] T. Hayashi, M. Nakano, and A. Yamaguchi, "Novel AoA estimation method using delay profile in downlink," in *2013 International Workshop on Antenna Technology (iWAT)*, March 2013, pp. 35–38.

[60] R. Irmer, H. Droste, P. Marsch, M. Grieger, G. Fettweis, S. Brueck, H. Mayer, L. Thiele, and V. Jungnickel, "Coordinated multipoint: Concepts, performance, and field trial results," *IEEE Communications Magazine*, vol. 49, no. 2, pp. 102–111, February 2011.

[61] M. Sawahashi, Y. Kishiyama, A. Morimoto, D. Nishikawa, and M. Tanno, "Coordinated multipoint transmission/reception techniques for LTE-advanced [coordinated and distributed MIMO]," *IEEE Wireless Communications*, vol. 17, no. 3, pp. 26–34, June 2010.

[62] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Processing Letters*, vol. 19, no. 2, pp. 71–74, Feb 2012.

[63] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, Oct 2010.

[64] M. Ben-Zid, *Recent Trends in Multi-user MIMO Communications*. London, UNITED KINGDOM: IntechOpen Limited, 2013.

[65] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the 1979 AFIPS National Computer Conference*. Monval, NJ, USA: AFIPS Press, 1979, pp. 313–317.

[66] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[67] T. Chen and K. Tsao, “User-friendly random-grid-based visual secret sharing,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 21, no. 11, pp. 1693–1703, Nov 2011.

[68] M. Ehdaie, T. Eghlidos, and M. R. Aref, “A novel secret sharing scheme from audio perspective,” in *2008 International Symposium on Telecommunications*, Aug 2008, pp. 13–18.

[69] Y. Miura and Y. Watanabe, “Security of (n, n)-threshold audio secret sharing schemes encrypting audio secrets,” in *2016 IEEE Statistical Signal Processing Workshop (SSP)*, June 2016, pp. 1–5.

[70] T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. New York, NY, USA: Wiley-Interscience, 2006.

[71] A. F. Serra, J. J. O. Bonafé, and M. Á. L. Rosas, “Modelling channel estimation error in LTE link level simulations,” in *COST IC1004 Cooperative radio communications for green smart environments: 3rd Scientific meeting*, Feb 2012, pp. 8–10.

[72] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[73] K. Zheng, S. Ou, and X. Yin, “Massive MIMO channel models: A survey,,” *nternational Journal of Antennas and Propagation*, vol. 2014, June 2014.

[74] Z. Luo and S. Zhang, “Dynamic spectrum management: Complexity and duality,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 57–73, Feb 2008.

[75] C. W. Tan, M. Chiang, and R. Srikant, “Fast algorithms and performance bounds for sum rate maximization in wireless networks,” *IEEE/ACM Transactions on Networking*, vol. 21, no. 3, pp. 706–719, June 2013.

[76] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. New York, NY, USA: Cambridge University Press, 2005.

[77] 3GPP, "NR; Physical channels and modulation," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.211, 09 2019, version 15.7.

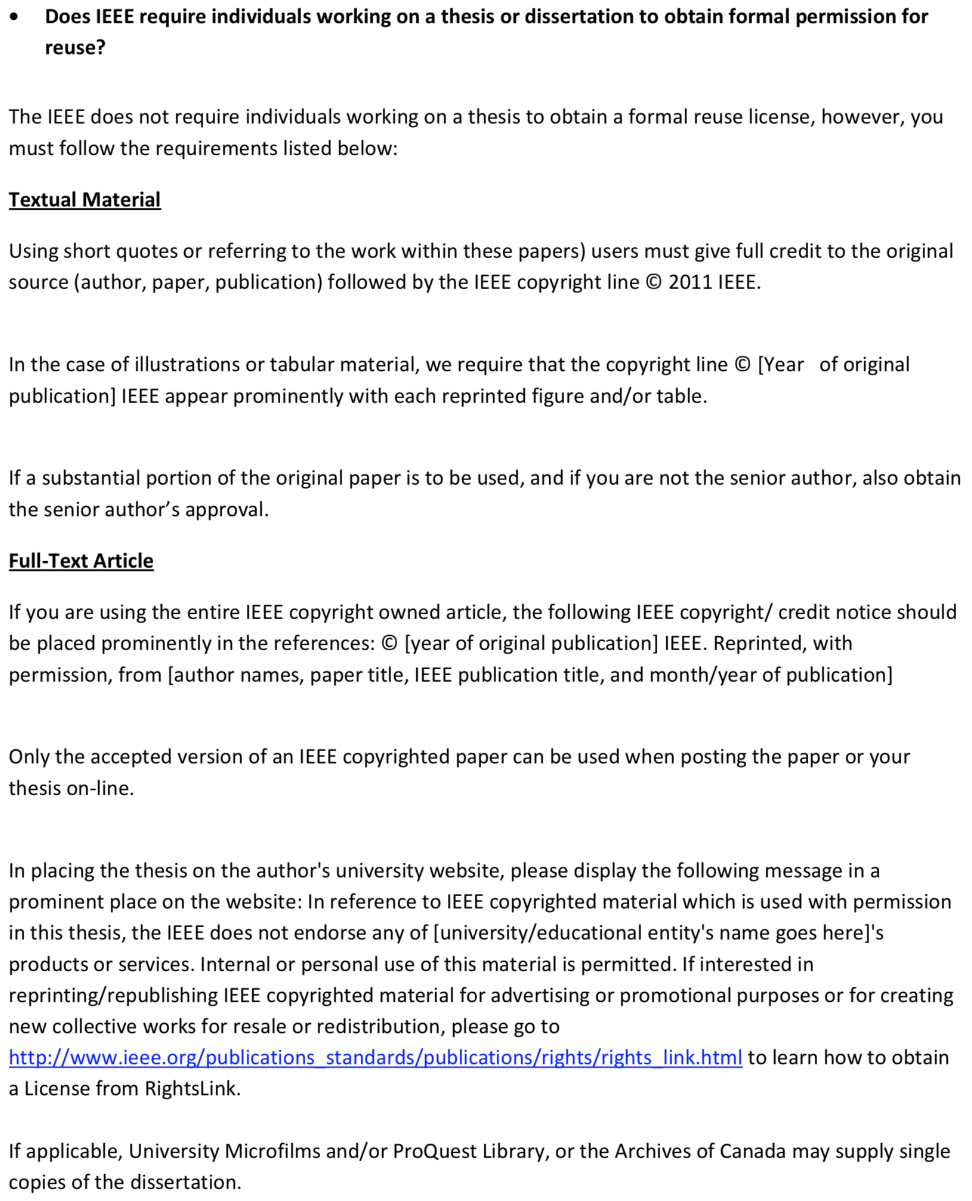
[78] ——, "NR; Physical layer procedures for control," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.213, 09 2019, version 15.7.

[79] L. Kundu, G. Xiong, and J. Cho, "Physical uplink control channel design for 5G new radio," 2018.

[80] S. Kay, *Fundamentals of Statistical Signal Processing I: Estimation theory*, ser. Prentice Hall Signal Processing Series. Prentice-Hall PTR, 1998.

Appendix A: Proof of Copyright Permissions

The permission below is for the use of materials in Chapter 3.



- **Does IEEE require individuals working on a thesis or dissertation to obtain formal permission for reuse?**

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you must follow the requirements listed below:

Textual Material

Using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.

In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.

If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Full-Text Article

If you are using the entire IEEE copyright owned article, the following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]

Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.

In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

About the Author

Received the B.Sc. degree in electrical engineering from Alexandria University, Alexandria, Egypt, in 2010, and the M.Sc. degree in electrical engineering from the same university, in 2014. He was a graduate assistant in the Wireless Communications and Signal Processing Group, University of South Florida, Tampa, FL, from 2014 to 2019. He was a research assistant in the department of electrical engineering at Qatar University, Doha, Qatar, from 2011 to 2014. He was also a research assistant in the department of electrical engineering at Alexandria University, Alexandria, Egypt, from 2010 to 2011. Currently, he is an algorithm developer with Intel Corporation, Santa Clara, CA. His current research interest is focused on physical layer design/signal processing for 5G networks and beyond.