MULTIPLE ANTENNA BASED PHYSICAL LAYER SECURITY WIRELESS SYSTEMS

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

MASTER OF SCIENCE

in Electronics and Communication Engineering

by
Özgecan Özdoğan ŞENOL

July 2017
İZMİR

We approve the thesis of **Özgecan Özdoğan ŞENOL**

Examining Committee Members:

Assist. Prof. Dr. Berna ÖZBEK
Department of Electrical and Electronics Engineering, İzmir Institute of Technology

Assoc. Prof. Dr. Barış ATAKAN
Department of Electrical and Electronics Engineering, İzmir Institute of Technology

Assist. Prof. Dr. Nalan ÖZKURT
Department of Electrical and Electronics Engineering, Yaşar University

11 July 2017

Assist. Prof. Dr. Berna ÖZBEK
Supervisor, Department of Electrical and Electronics Engineering
İzmir Institute of Technology

Prof. Dr. Enver TATLICIOĞLU
Head of the Department of
Electrical and Electronics Engineering

Prof. Dr. Aysun SOFUOĞLU
Dean of the Graduate School of
Engineering and Sciences

ACKNOWLEDGMENTS

I would firstly like to express my gratitude to my supervisor Assist. Prof. Dr. Berna Özbek for her guidance, support, and motivation during this study and preparation of this thesis.

I would also like to express my gratitude to my committee members Assoc. Prof. Dr. Barış Atakan and Assist. Prof. Dr. Nalan Özkurt for their contributions. A special thanks should be extended to Assoc. Prof. Dr. Güneş Karabulut Kurt for her meticulous review and useful advices.

İzmir Institute of Technology, which I work as a research assistant in Department of Electrical and Electronics Engineering, deserves my gratitude for supporting me from the day that I start working. I had the opportunity to work in a friendly environment with knowledgeable and helpful researchers. Among my colleagues, I would like to express special gratitude to Başak Esin Köktürk Güzel and Oktay Karakuş for their steady support and care what makes it possible to always persist in my endeavors.

I want to thank my husband Vedat Şenol for his never-ending love, support and understanding. Without him, this study would be more and more difficult. I would also like to thank my family for their support and sympathy. They deserve every good intention and I am thankful to my father İsmet Özdoğan, my mother Hanife Özdoğan and my sister Özden Özdoğan.

This thesis is supported by The Scientific and Technical Research Council of Turkey (TUBITAK) under the grant of 114E626 Tübitak-Ardeb-1005 project.

ABSTRACT

MULTIPLE ANTENNA BASED PHYSICAL LAYER SECURITY WIRELESS SYSTEMS

In the last decade, the demand for wireless services increases at unprecedented rates. Due to the inherent open nature of radio propagation, wireless transmission is vulnerable to various attacks despite its popularity. Therefore, communication security in wireless networks is becoming more critical than ever. Conventionally, cryptographic techniques are deployed on upper layers of network protocols as a solution. As a complement to the traditional cryptographic techniques, physical layer (PHY) security exploits the characteristics of wireless channels to enable secure wireless communications. The aim is to limit the amount of information that can be extracted by any unauthorized users via utilizing inherent randomness of noise and communication channels. The design of PHY security schemes is not based on the premise that eavesdropper has limited computational power contrary to upper layer secrecy techniques. In fact, the eavesdropper may have infinite computational power. Nevertheless, secure communication can be achieved by the combination of appropriate coding and transmit precoding design with the usage of available channel state information. PHY security methods can work independently from upper layer encryption techniques. Thus, PHY security techniques can be used to leverage the secrecy of already existing communication systems.

In this thesis, PHY security enhancement mechanisms, especially in multiuser multiple antenna systems with a limited feedback link are investigated. Four different system models under secrecy consideration with different channel conditions including quasi-static fading channels, temporally correlated fading channels are presented. In order to disrupt the reception of any potential eavesdropper, artificial noise (AN) beamforming scheme is employed. The effects of lack of perfect channel state information (CSI) at the transmitter and the AN leakage that is caused by limited CSIT are analyzed. The thesis proposes a reduction in feedback load using receiver side selection criterion with special codebook design and appropriate beamforming. Our approach is capable of enhancing the security of wireless communications by selecting the users with favorable channel conditions and quantizing channel direction information (CDI) by a special codebook. Also, inter-user interference is utilized as a jamming method when eavesdropper's CSI unknown by the transmitter. Simulation results demonstrate the feasibility of the proposed PHY security mechanisms by examining the achievable secrecy rates.

ÖZET

KABLOSUZ SİSTEMLERDE ÇOKLU ANTEN TABANLI FİZİKSEL KATMAN GÜVENLİĞİ

Son on yılda, kablosuz hizmetler için talep benzeri görülmemiş oranlarda artmaktadır. Günümüzde kablosuz iletişim hayatımızın ayrılmaz bir parçasıdır. Kablosuz iletim popülaritesine rağmen telsiz yayılımının doğası gereği saldırılara karşı savunmasızdır. Bu nedenle, kablosuz ağlarda iletişim güvenliği her zamankinden daha kritik hale gelmektedir. Geleneksel olarak, şifreleme teknikleri ağ protokollerinin üst katmanlarında güvenlik amacıyla kullanılır. Geleneksel şifreleme tekniklerine bir tamamlayıcı olarak fiziksel katman güvenliği, kablosuz iletişimin güvenliğini sağlamak için kablosuz kanalların rastlantısallık özelliklerini kullanır. Amaç, gizli dinleyicilerin ele geçirebileceği bilgi miktarını iletişim kanallarına özgü rastlantısallığı kullanarak sınırlamaktır. Fiziksel katman güvenliği tasarımı, üst katmanlardaki güvenlik tekniklerinin aksine gizli dinleyicinin sınırlı hesaplama gücüne sahip olduğu öncülüne dayanmamaktadır. Aksine, gizli dinleyici sonsuz bir hesaplama gücüne sahip olabilir. Güvenli iletişim uygun kod kitapçığı, hüzmeleyici tasarımı ve ayrıca mevcut kanal durumu bilgisinin kullanımı ile sağlanabilir. Fiziksel katman güvenlik yöntemleri, üst katman şifreleme tekniklerinden bağımsız olarak çalışabilir. Böylelikle, mevcut iletişim sistemlerinin gizliliğini arttırmak için fiziksel katman güvenlik teknikleri kullanılabilir.

Bu tezde, özellikle sınırlı geri bildirimli çok kullanıcılı çoklu antenli sistemlerde fiziksel katman güvenlik geliştirme mekanizmaları incelenmiştir. Durağan ve zamanla ilintili sönümlü kanallar gibi farklı kanal koşullarına sahip gizlilik kaygısı altında çalışan dört farklı sistem modeli incelenmiştir. Herhangi bir potansiyel gizli dinleyicinin algısını bozmak için yapay gürültü hüzlemeyicisi kullanılmıştır. Vericinin mükemmel kanal durum bilgisine sahip olamamasının ve sınırlı kanal durum bilgisinin neden olduğu yapay gürültü sızıntısının etkileri analiz edilmiştir. Tez, özel kod kitapçığı tasarımı ve uygun hüzmeleyici ile birlikte alıcı tarafında seçim kriterini kullanarak geri besleme yükünde bir azalma önermektedir. Yaklaşımımız, uygun kanal koşullarına sahip kullanıcıları seçerek ve kanal yönü bilgilerini özel bir kod kitapçığıyla nicemleyerek kablosuz iletişim güvenliğini güçlendirebilmektedir. Ayrıca, verici tarafında gizli dinleyicinin kanalı bilinmediğinden, kullanıcılar arası girişim bir güvenlik yöntemi olarak kullanılmıştır. Benzetim çalışmaları sonuçları, erişilebilir güvenlik kapasitelerini inceleyerek önerilen fiziksel güvenlik mekanizmalarının uygulanabilirliğini göstermektedir.

LIST OF FIGURES

Figure **Page**

LIST OF ABBREVIATIONS

AN	Artificial Noise
AWGN	Additive White Gaussian Noise
BCCM	Broadcast Channel with Confidential Messages
CDI	Channel Direction Information
CSI	Channel State Information
CSIT	Channel State Information at Transmitter
CQI	Channel Quality Information
DMRS	Demodulation Reference Symbols
ECSIT	Channel State Information of Eavesdropper at Transmitter
GSVD	Generalized Singular Value Decomposition
MISO	Multiple Input Single Output
MIMO	Multiple Input Multiple Output
MMSE	Minimum Mean Square Error
PHY	Physical Layer
RVQ	Random Vector Quantization
SINR	Signal to Interference plus Noise Ratio
SNR	Signal to Noise Ratio
ZFBF	Zero Forcing Beamforming

CHAPTER 1

INTRODUCTION

The fundamental characteristics of wireless medium present different challenges in achieving secure communications in the presence of unauthorized receivers. Privacy and confidentiality of transmitted information are vulnerable to interception of potential security threats due to the broadcast nature of radio signal propagation. In today's world, we experience a wireless revolution. Demands for wireless technologies and requests for higher data rates are continuously increasing. Wireless communication plays an integral part in our lives. Widespread use of the technologies like Wireless Local Area Networks, Bluetooth and Cellular Networks, raises the importance of security problem. Not only for public applications, the requirement of secrecy for applications concerning governmental, medical information, e-banking, and e-commerce also becomes more and more vital.

The adversarial user commonly modeled in two basic ways. It can be modeled as either an unauthorized receiver that maliciously tries to attain information from the signal of the intended user without being detected or a transmitter that tries to degrade the capacity of legitimate user via jamming. The first model is generally known as passive eavesdropper and the second one refers to active eavesdropper. The secrecy requirements exist that are presented in wireless networks against these threats including confidentiality and authentication. Confidentiality ensures that eavesdropper can not read confidential messages. Authentication ensures that receivers are able to sense transmission origin and any attacker will not be able to impersonate as the message source.

In existing communication systems, these security tasks are issued mostly by the upper layers of network protocol. Conventionally, complexity based cryptographic methods have been used to provide secrecy. However, this raises problems such as key distribution and high computational complexity (Schneier, 1996), (Schneier, 1998). Besides, all cryptographic measures are based on assumption that it is computationally infeasible to decipher them without knowledge of the secret key. As a complement to the traditional cryptographic techniques, PHY security exploits the characteristics of wireless channels to enable secure wireless communications. The essential premise of PHY security techniques is to facilitate the transmission of confidential messages over a wireless medium in the presence of eavesdroppers without relying on higher layer encryption. The aim is to limit the amount of information that can be extracted by any unauthorized users via utilizing inherent randomness of noise and communication channels. In order to achieve this target, PHY security utilizes two primary techniques.

A secret key may be generated via exploiting the wireless transmission medium randomness. As a second approach, It can be done by the transmit coding strategies without secret key generation. The design of PHY security schemes is not based on the premise that eavesdropper has limited computational power contrary to traditional methods. In fact, the eavesdropper may have infinite computational power. Nevertheless, secure communication can be achieved by the combination of appropriate coding and transmit precoding design. PHY security methods can work independently from upper layer encryption techniques. Thus, PHY security techniques can be used to leverage the secrecy of already existing communication systems.

1.1. Motivations

In this section, the motivations of this thesis are presented considering PHY security challenges in multiuser multiple antenna systems with limited feedback channels.

Over the last years, the interest in high data rate transmission has significantly increased. Multiple-input multiple-output (MIMO) antenna configurations are commonly used to meet this request in emerging wireless networks, since equipping multiple antennas at transmitters and receivers can achieve increased diversity and multiuser gains. In the aspect of PHY security, multiple antenna techniques have been proposed to improve secrecy performance via taking the advantage of spatial degrees of freedom. MIMO systems can enhance the received signal power at legitimate receivers and degrade the received signal quality at eavesdropper concurrently. This can be accomplished by utilizing proper beamforming strategies at the transmitter side.

Among various PHY techniques reported in the literature, multiple antenna techniques may be most effective methods in improving secrecy capacity. However, the success of these techniques almost completely depends on the availability of CSI, by reason that the transmitter designs the beamformer according to present CSI. In practical communication systems, it is hard to acquire even CSI of legitimate users perfectly since, the feedback channel is limited. In order to have CSI at transmitter, the receiver estimates and sends its CSI back to the transmitter. It is not possible to send perfect CSI back to transmitter since it requires infinite amount of bandwidth. Thus, in this thesis the sender is constrained to interpret available limited CSI. In order to reach secure wireless communications goal, the multiple antenna techniques and beamforming schemes with limited feedback are studied.

1.2. Research Objectives

Due to the fact that wireless transmission is vulnerable to interception of unauthorized receivers, the main research objective of this thesis is to develop PHY security enhancement mechanisms especially in multiuser MIMO systems with limited available feedback.

More specifically, our aims for the multiuser MIMO secure wireless communications are to mitigate noise leakage and interference on other users while reaching multiplexing gain. In existing transmitter beamforming schemes in literature, masking the information signal with artificially generated noise to disrupt reception of any possible has been highly studied in Goel and Negi (2008). In this approach, if CSIT of intended users are perfectly available, the transmitter can inject AN into the null space of channel of legitimate users without affecting intended users. Thus, it disrupts the reception of eavesdropper that maliciously try to attain information from legitimate users signal. The transmit power is partitioned between the information signal and AN to mask the desired signal from any potential eavesdropper. When the transmit power is allocated properly, a positive secrecy capacity can be guaranteed even if eavesdropper has better channel conditions than the legitimate user. We are interested in the case which legitimate users also receive AN since in general only quantized CDI is available at the transmitter due to rate limitations on the feedback channel. This case is referred as AN leakage problem. In this thesis, we aim to mitigate the AN leakage on intended users' channel.

Additionally, one of our objectives is to reduce feedback load using appropriate transmit beamforming mechanisms. In order to increase secrecy rate and overcome the noise leakage problem, a large number of quantization bits should be used. As the number of employed antennas increases, the total feedback load even become larger. This situation necessitates the use of codebook that quantizes channel information. Codebook based transmission schemes that the receiver sends back the only index of the optimum beamformer by a few bits has commonly adopted in practice. Generally, a suitable codebook takes channel statistics into account (Love et al., 2003), (Mukkavilli et al., 2003). In this thesis, we consider different codebook designs for different channel conditions including quasi-static fading and temporally correlated fading channels.

On the other hand, increasing number of active users also increases the overhead in multiuser communications. We aim to construct receiver side user selection mechanism with special codebook design to achieve secure multiuser communications.

1.3. Thesis Outline

The rest of this thesis is organized as follows:

Chapter 2 describes the overall background information related to and used in the following chapters of the thesis. In Section 2.1, the brief history of PHY security is presented. The Section 2.2 introduces the secure multiple antenna techniques including the generalized singular value decomposition beamforming, artificial noise beamforming and zero forcing beamforming. The Section 2.3 contains the quantization of CSI and beamforming techniques for limited CSI. Besides, the design of differential codebook is also presented.

In Chapter 3, two different secure single user MISO system models with different channel conditions are studied. In Section 3.1, the system model with quasi-static fading channel is investigated. In Section 3.2, the problem of secure single user MISO systems over temporally correlated channels is studied. The simulation results are provided for both system models.

In Chapter 4, a PHY security enhancement using rotated codebook design and semi-orthogonal user selection at receiver side is presented. The Section 4.1 provides a transmission scheme that utilizes inter-user interference as a jamming method. The system model includes a single antenna eavesdropper with unknown CSI at transmitter. The Section 4.4 consists an multiple antenna eavesdropper corresponds to an alliance of geographically dispersed but perfectly colluding single antenna eavesdroppers. In that case artificial noise beamforming employed along with rotated codebook and receiver side user selection instead of inter-user interference jamming. The simulation results demonstrate the feasibility of the system's security by using the proposed methods.

Finally, Chapter 5 concludes all the key information appeared in previous chapters. Also, the future works are included.

CHAPTER 2

BACKGROUND

This chapter provides a background for the research that is examined in this thesis. In the first section, a brief history of PHY security is given. In the second section, secure multiple antenna technologies are reviewed. A literature survey of single user and multi-user wireless network with security issues is conducted. Various precoding methods for different types of CSI availability at the transmitter are presented. In the third section,the effect of quantization of CSI on secure communication is provided.

2.1. Brief History of Physical Layer Security

The origin of PHY security can be traced back to Shannon's information theoretical analysis on secrecy systems (Shannon, 1949). Afterwards, Wyner introduced the concept of secrecy capacity and wiretap-channel model as a framework (Wyner, 1975). It consists of three nodes, transmitter (Alice), receiver (Bob) and eavesdropper (Eve). This model characterizes a communication system under secrecy constraint. In this pioneering work, Wyner defined secrecy capacity as the maximum amount of information that can be reliably transmitted from a transmitter to the intended receiver. This work only considers the degraded channels. Indeed, Wyner only showed that it is possible to perform secure communications in degraded broadcast channels.

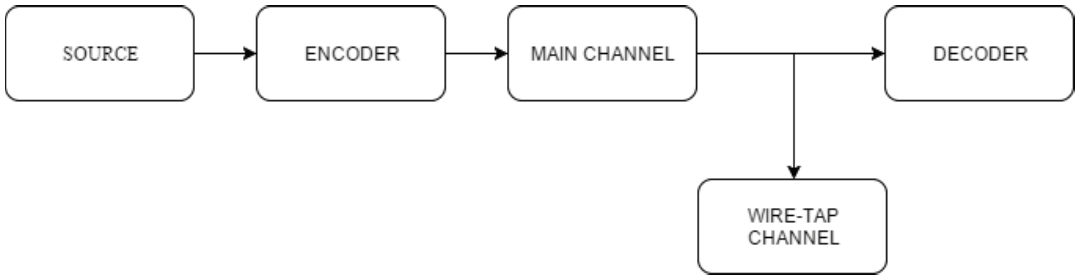

Figure 2.1. Wyner's wire-tap model

Early investigations on PHY security (Carleial and Hellman, 1977), (Yamamoto, 1989), (Yamamoto, 1991) were mainly inspired by the concept of entropy and equivocation. In sub-

sequent studies, various channel models were analysed in the information theoretical point of view. In (Csiszar and Korner, 1978), authors generalized the wire-tap channel model to broadcast channel with confidential messages. Introduction of PHY-security in Gaussian channels (Leung-Yan-Cheong and Hellman, 1978), small scale fading channels (Liang et al., 2008), (Gopala et al., 2008), multi-antenna channels (Shafiee and Ulukus, 2007), (Khisti and Wornell, 2010) and relay channels (Lai and Gamal, 2008), (Dong et al., 2010) followed these works.

In the existing communication systems, these security tasks are issued mostly by the upper layers of network protocol. Conventionally, complexity based cryptographic methods have been used to provide secrecy. However, this raises problems such as key distribution and high computational complexity (Schneier, 1996), (Schneier, 1998). Besides, all cryptographic measures are based on assumption that it is computationally infeasible to decipher them without knowledge of the secret key. As a complement to the traditional cryptographic techniques, PHY security exploits the characteristics of wireless channels to enable secure wireless communications. The essential premise of PHY security techniques is to facilitate the transmission of confidential messages over a wireless medium in the presence of eavesdroppers. The aim is to limit the amount of information extracted by any unauthorized users via utilizing inherent randomness of noise and communication channels. In order to achieve this target, PHY security utilizes two primary techniques. A secret key may be generated via exploiting the wireless transmission medium randomness. As a second approach, the transmit precoding strategies are developed without secret key generation. The design of PHY security schemes is not based on the premise that eavesdropper has limited computational power contrary to traditional methods. In fact, the eavesdropper may have infinite computational power. Nevertheless, secure communication can be achieved by the combination of appropriate coding and transmit precoding design and also the usage of available channel state information. Physical layer security methods can work independently from upper layer encryption techniques. Thus, PHY security techniques can be used to leverage the secrecy of already existing communication systems.

2.2. Secure Multi-Antenna Technologies

The main performance metric of PHY security is secrecy rate and it can be measured instantaneously, asymptotically or statistically. Basically, it is the difference between channel capacities of legitimate user and eavesdropper (Wyner, 1975). In order to enhance the secrecy rate, the signal to noise ratio (SNR) at Eve must be decreased while increasing the SNR at the Bob. This optimization problem can not be solved by simply increasing the transmit power,

since it increases SNR at the Eve simultaneously.

Multiple antenna techniques are extensively studied in PHY security configurations, (Liu and Shamai, 2009), (Shafiee et al., 2009), (Liu and Shamai, 2009), (Oggier and Hassibi, 2011), (Hong et al., 2013), (Lin et al., 2014). More specifically, the research that was conducted in (Huang and Swindlehurst, 2011), (Du et al., 2015) focuses on multiple antenna relay assisted secure communications. Also, (Dong et al., 2009), Yang et al. (2013) concentrate on multiple antenna jamming techniques and (Zhu et al., 2016), (Chen et al., 2016) studied on massive MIMO systems. Additionally, (Valliappan et al., 2013), (Hafez and Arslan, 2015), (Yusuf and Arslan, 2015) presented directional modulation in multiple antennas.

The extensive interest to secure multiple antenna techniques stems from its potential of enhancing secrecy rates. Employing multiple antennas enables to achieve degrees of freedom that can be used against eavesdroppers. In order to reach high secrecy rates, proper beamforming schemes should be utilized in multiple antenna wireless communications. The introduction of Demodulation Reference Symbols (DMRS) in 3GPP LTE standard allows transmitter to use various MIMO precoding strategies. Also, arbitrary MIMO precoding is enabled by IEEE 802.11ac. Thus, PHY security MIMO beamforming techniques can be adapted to current developments of wireless technologies without major changes (Mukherjee et al., 2014).

This section is devoted to introduce various beamforming schemes with multiple antenna technologies. The remainder of this section is organized as follows. In Section 2.2.1, PHY-Security multiple antenna techniques and precoding methods for single user systems are reviewed. In Section 2.2.2, a literature survey on the secure multi-user multiple antenna techniques is conducted.

2.2.1. Single User Multiple Antenna and Precoding Strategies

Single user multiple antenna network refers to system model that consists three nodes: Alice with N_t antennas, Bob with single antenna and Eve with N_e antenna. Alice corresponds to the transmitter where Bob corresponds to the legitimate user that Alice intends to send confidential information signal. Also, Eve is the eavesdropper that tries to attain information from the signal of legitimate user Bob.

In the development of precoding strategies, one of the main consideration is type of available CSI. In this section, related beamforming techniques for point-to-point MIMO systems according to type of available CSI are reviewed. In Section 2.2.1.1, the precoding method that requires CSI at the transmitter (CSIT) of both Bob and Eve is considered. In Section 2.2.1.2, the beamforming scheme that does not require CSI of Eve at the transmitter is reviewed.

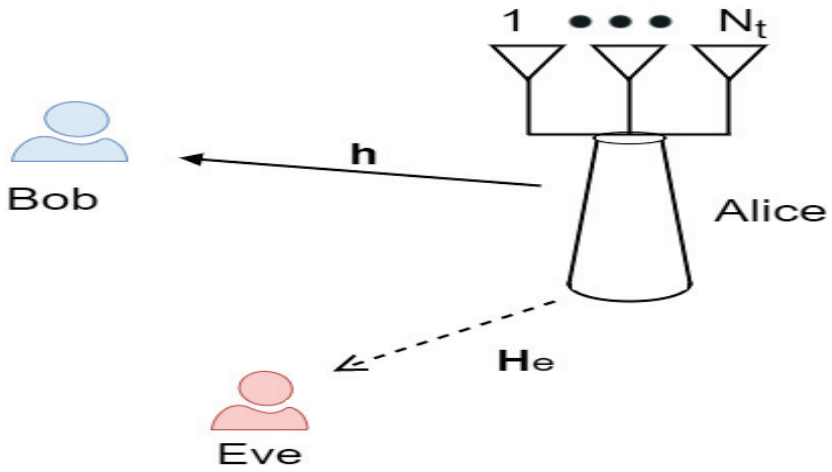

Figure 2.2. An illustration of single user multiple antenna system model with Eve

2.2.1.1. Generalized Singular Value Decomposition Beamforming

In Generalized Singular Value Decomposition (GSVD) based beamforming, the main channel and wiretap channel can be divided into parallel channels (Khisti and Wornell, 2010). In this scheme, perfect CSIs of both Bob and Eve are required.

The (λ, Ψ) pair is the generalized eigenvalue-eigenvector pair, if they satisfy the following criterion,

$$\mathbf{A}\Psi = \lambda\mathbf{B}\Psi \tag{2.1}$$

where $\mathbf{A} \in \mathbb{C}^{n\times n}$ is a Hermitian matrix and $\mathbf{B} \in \mathbb{C}^{n\times n}$ is a positive definite matrix. The eigenvectors of pair $(\mathbf{A}, \mathbf{B})$ are the stationary point solutions of Rayleigh Quotient. More specifically, the largest eigenvalue is the maximum of Rayleigh Quotient and it is defined as,

$$\lambda_{max}(\mathbf{A}, \mathbf{B}) = \max_{\Psi\in\mathbb{C}^{n\times 1}} \frac{\Psi^H\mathbf{A}\Psi}{\Psi^H\mathbf{B}\Psi}. \tag{2.2}$$

The optimum eigenvector Ψ_{max} gives the $\lambda_{max}(\mathbf{A}, \mathbf{B})$. If transmitter can acquire the CSIs of both Eve and Bob, the secrecy capacity can be computed as (Khisti and Wornell, 2010),

$$R(P) = \left\{\log\lambda_{\max}\left(\mathbf{I} + P\mathbf{h}\mathbf{h}^H, \mathbf{I} + P\mathbf{H}_e^H\mathbf{H}_e\right)\right\}^+ \tag{2.3}$$

where $\mathbf{h} \in \mathbb{C}^{N_t\times 1}$ is the channel vector of Bob and $\mathbf{H}_e \in \mathbb{C}^{N_e\times N_t}$ is the channel matrix of Eve. The P is the total transmit power. The largest generalized eigenvalue Ψ_{max} corresponds to $(\mathbf{I} + P\mathbf{h}\mathbf{h}^\dagger, \mathbf{I} + P\mathbf{H}_e^\dagger\mathbf{H}_e)$ pair that maximizes the Rayleigh Quotient as,

$$\lambda_{\max}(\mathbf{I} + P\mathbf{h}\mathbf{h}^H, \mathbf{I} + P\mathbf{H}_e^H\mathbf{H}_e) = \max_{\Psi \in \mathbb{C}^{N_t \times 1}} \frac{\Psi^H(\mathbf{I} + P\mathbf{h}\mathbf{h}^H)\Psi}{\Psi^H(\mathbf{I} + P\mathbf{H}_e^H\mathbf{H}_e)\Psi}. \tag{2.4}$$

The received signals at receiver and eavesdropper are,

$$y = \mathbf{h}^H\mathbf{x} + n \tag{2.5}$$

$$\mathbf{y}_e = \mathbf{H}_e\mathbf{x} + \mathbf{n}_e \tag{2.6}$$

where $\mathbf{x} \in \mathbb{C}^{N_t \times 1}$ is the transmitted signal vector that has power $\mathbb{E}\left\{\|\mathbf{x}\|^2\right\} = P$. Since the optimum beamforming direction is Ψ_{max}, the $\mathbf{x} = \Psi_{max}s$ where s is the information bearing signal. The additive white Gaussian noises (AWGN) at legitimate receiver and eavesdropper respectively, n $\mathcal{CN}(0, \sigma^2)$ and $\mathbf{n}_e$ $\mathcal{CN}(0, \sigma_e^2\mathbf{I}_{N_e})$.

In the case of limited feedback, quantized versions of $\mathbf{h}$ and $\mathbf{H}_e$ i.e, $\hat{\mathbf{h}}$ and $\hat{\mathbf{H}}_e$ are present at transmitter, respectively. Thus, the direction of beamforming is not along Ψ_{max} anymore, due to the quantization error and it causes a secrecy degradation. Without available CSI of Eve (ECSIT), sub-optimal SVD precoding scheme was discussed in (Shafiee and Ulukus, 2007). In subsequent studies, optimal power allocation for GSVD beamforming and its performance comparison with nonlinear dirty paper coding was presented in (Fakoorian and Swindlehurst, 2011), (Fakoorian and Swindlehurst, 2012).

2.2.1.2. Artificial Noise Beamforming

In order to guarantee positive secrecy rate without ECSIT at the transmitter, artificial noise (AN) assisted beamforming technique was presented by (Negi and Goel, 2005; Goel and Negi, 2008). In this method, information signal is masked with AN signal that is injected in the direction of legitimate user's null space. This masked precoding scheme ensures positive secrecy rates, even if eavesdropper has better channel conditions than legitimate user's channel.

Consider a secure point-to-point multiple antenna system model that consists of Alice with N_t, Bob and Eve are equipped with single antenna. The transmitted signal is,

$$\mathbf{x} = \mathbf{w}s + \mathbf{Q}\mathbf{a} \tag{2.7}$$

where s is the information signal and $\mathbf{a} \in \mathbb{C}^{(N_t-1)\times 1}$ is the AN signal vector. The AN vector $\mathbf{a}$ is a random Gaussian vector that each element has distribution $\mathcal{CN}(0, \sigma_a^2)$. Also, $\mathbf{w} \in \mathbb{C}^{N_t \times 1}$ is the beamforming vector in the direction of Bob's channel. AN beamforming

matrix $\mathbf{Q} \in \mathbb{C}^{N_t \times N_t - 1}$ is generated in the null space of $\mathbf{w}$, i.e. $\|\mathbf{w}^H \mathbf{Q}\| = 0$. The AN beamformer $\mathbf{Q}$ forms an orthonormal basis for AN subspace. Figure 2.3 illustrates the geometric interpretation of beamformers $\mathbf{w}$ and $\mathbf{Q}$.

The beamformer matrices $\mathbf{w}$ and $\mathbf{Q}$ are generated according to available CSI at the transmitter. If Alice has perfect knowledge regarding intended user's channel and there is no information about Eve CSI, the received signals at Bob and Eve can be expressed as,

$$y = \mathbf{h}^H \mathbf{w} s + n, \tag{2.8}$$

$$y_e = \mathbf{h}_e \mathbf{w} s + \mathbf{h}_e \mathbf{Q} \mathbf{a} + n_e, \tag{2.9}$$

respectively, where $\mathbf{h}_e \in \mathbb{C}^{1 \times N_t}$ channel vector of single antenna Eve and n_e is the AWGN with distribution $\mathcal{CN}(0, \sigma_e^2)$. As given in Equation (2.8), legitimate user can eliminate artificial noise when perfect CSI is available at Alice. However in Equation (2.9), reception of the eavesdropper is disrupted by AN to reduce its capacity given in Equation (2.11)

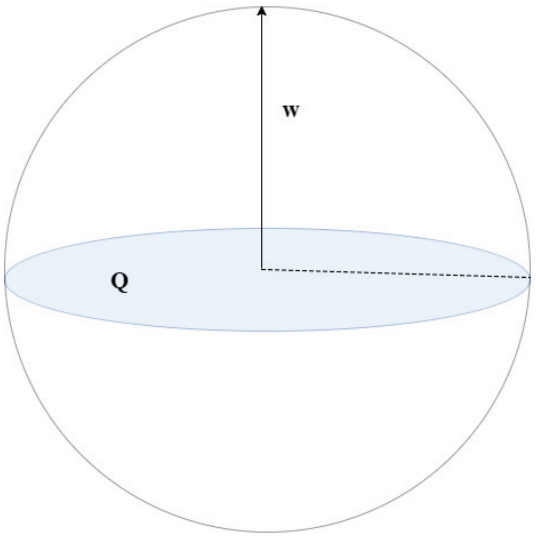

Figure 2.3. A geometric interpretation of beamforming directions

The beamformer $\mathbf{w}$, can be constructed as,

$$\mathbf{w} = \frac{\mathbf{h}}{\|\mathbf{h}\|}. \tag{2.10}$$

Thus, the term $|\mathbf{h}^H \mathbf{Q}|$ is equal to zero and Bob is not affected by AN. In this beamforming scheme, the total transmit power P is partitioned between the message signal and the

AN signal to jam eavesdropper. The power that is allocated to transmit information signal is denoted as $P_s = \alpha P$. Likewise, the power that is spent for artificial noise signal can be written as $P_a = \frac{(1-\alpha)P}{N_t-1}$ where the parameter α is responsible for power allocation. Thus, reception of eavesdropper is disrupted and secrecy rate is maximized with optimum power allocation parameter α. In perfect Bob CSI case, optimum power allocation paramater is $\alpha = 0.5$ that corresponds to equal power partition for information and AN signals (Lin et al., 2011). With perfect knowledge of CSI of legitimate user, it is possible to achieve arbitrarily large secrecy rate by increasing total transmit power (Xiong et al., 2012), (Zhou and McKay, 2010). Then, the secrecy rate can be written as,

$$R(\alpha) = \max\left(\mathbb{E}\{log_2(1+\gamma_b)\} - \mathbb{E}\{log_2(1+\gamma_e)\}\right)^+ \tag{2.11}$$

where γ_b and γ_e are correspond to SNRs at Bob and Eve respectively;

$$\gamma_b = \frac{\alpha P|\mathbf{h}^H\mathbf{w}|^2}{\sigma^2}, \tag{2.12}$$

$$\gamma_e = \frac{\alpha P|\mathbf{h}_e\mathbf{w}|^2}{\frac{(1-\alpha)P}{N_t-1}||\mathbf{h}_e\mathbf{Q}||^2 + \sigma_e^2}. \tag{2.13}$$

In literature, more complex exhaustive search algorithms also investigated. (Gerbracht et al., 2012) considered a single-stream beamforming and the use of AN in the null space of the main channel. In (Li et al., 2013), authors presented a transmit optimization approach to tackle the secrecy optimization problems. (Li and Ma, 2011) addressed the transmit covariance optimization for secrecy-rate maximization problem of the system with multiple antenna eavesdroppers. This nonconvex optimization problem was investigated via semidefinite program. Also, energy-efficient precoder design in a three-node multiple input multiple outpur-t wiretap channel was studied in (Zhang et al., 2014).

2.2.2. Multiuser Multiple Antenna Strategies

In a multiuser system, different wireless channels fade independently among the users, the transmitter or receiver can concurrently transmit or receive more than one user. The multiuser multiple antenna systems such as broadcast or multiple access channels can be adopted to information theoretic security approach.

If Alice transmits data to the users, the channel is referred as a downlink or broadcast channel. Conversely, when the users transmit data to base station, the channel is referred as an uplink or multiple access channel. The broadcast channel was introduced by Cover in early 1970's (Cover, 1972), whereas the multiple access channel dates back to Shannon.

The Wyner's wire-tap channel model was extended to the broadcast channel with confidential messages (BCCM) in (Csiszar and Korner, 1978). BCCM corresponds to a network that each information signal must be kept confidential from all other unintended receivers. In this model, all these unintended nodes are seen as eavesdroppers. These eavesdroppers are referred as internal eavesdroppers. Also, the system model that do not require to keep messages secret from all legitimate downlink users but only from external eavesdroppers is referred as Wire-tap broadcast channel. The secrecy rate regions and optimal power allocation for BCCM model was studied by references (Weingarten et al., 2006), (Liang et al., 2008), (Liu and Poor, 2009), and (Ly et al., 2010). Secure broadcasting for more than two users were investigated in (Khisti et al., 2008), (Bagherikaram et al., 2013). The considered system models include one legitimate receiver and try to communicate more than one other legitimate users under secrecy considerations. Also, (Chia and Gamal, 2012) studied three receiver BCCM and provided inner and outer bounds for this network.

The AN beamforming techniques can be used in multiuser MIMO systems to improve secrecy sum rates. In (Mukherjee and Swindlehurst, 2009b), authors selectively degraded the eavesdropper's channel with generating AN that is orthogonal to the desired receivers. Also, the confidentiality provided by zero-forcing and optimal minimum-power beamforming designs for the broadcast channel, and optimal minimum mean square error (MMSE) beamformers for the multicast channel were analyzed. In (Liao et al., 2010), authors proposed to jointly optimize the beamforming vector and the AN covariance matrix by minimizing the total transmit power subject to a target signal-to-interference-plus-noise ratio (SINR) constraint on Bob and limited SINR constraints on all Eves. Other precoding strategies for broadcast channels were also investigated in the literature. In (Fakoorian and Swindlehurst, 2013), the optimality of linear precoding for the two-receiver MIMO Gaussian BCCMs was studied. The performance of GSVD and dirty paper precoding for BCCM was compared in (Fakoorian and Swindlehurst, 2011). (Geraci et al., 2012) analysed secrecy sum rate for multi user MIMO regularized channel inversion beamforming scheme.

In order to maximize the secrecy sum capacity of the downlink MIMO system while achieving multiuser diversity, it is necessary to select the best combinations of legitimate users. User selection schemes under secrecy considerations are investigated in (Mukherjee and Swindlehurst, 2009a), (Yanase and Ohtsuki, 2010), (Li et al., 2016). In (Krikidis and Ottersten, 2013), authors proposed to apply opportunistic scheduling with orthogonal random beamforming. (Deng et al., 2016) considered a user selection scheme for secure uplink transmission. The closed-form expressions of the achievable ergodic secrecy sum rates in the high and low SNR regimes were presented. (Liu et al., 2014) studied the beamforming and user selection problem in multicast MISO wiretap-channel to maximize the minimum secrecy-outage rate of Bobs and give an iterative successive convex approximation algorithm.

2.2.2.1. Zero Forcing Beamforming

It is a practical interest to design MIMO multiuser systems with low complexity and minimum CSIT requirement. Zero forcing beamforming (ZFBF) is a suboptimal linear precoding method with low computational complexity. In this method, the precoders are chosen to avoid interference among users. The precoding matrix is designed to be the pseudo inverse of the channel matrix of the selected users. ZFBF is power inefficient when the number of users are low. However, it is asymptotically optimal when the number of users approaches to the infinity.

If the number of users K less than number of transmitter antennas N_t and assuming that perfect CSI is available, the ZFBF matrix $\mathbf{F} \in \mathbb{C}^{N_t \times K}$ can be determined as,

$$\mathbf{F} = \nu \mathbf{H}^H (\mathbf{H}\mathbf{H}^H)^{-1} \tag{2.14}$$

where $\mathbf{H} = [\mathbf{h}_1, \ldots, \mathbf{h}_k, \ldots, \mathbf{h}_K]^H$ is the joint channel matrix of K users where $\mathbf{h}_k \in \mathbb{C}^{N_t \times 1}$ and $\mathbf{H} \in \mathbb{C}^{K \times N_t}$. Also, $\mathbf{f}_k \in \mathbb{C}^{N_t \times 1}$ denotes the column of $\mathbf{F}$ where $\mathbf{F} = [\mathbf{f}_1, \ldots, \mathbf{f}_k, \ldots, \mathbf{f}_K]$.

The term ν is the power constant as,

$$\nu = \frac{1}{\sqrt{\mathrm{tr}\,(\mathbf{H}\mathbf{H}^H)^{-1}}}. \tag{2.15}$$

When the number of users K is equal to the number of transmit antennas, the ZFBF matrix is proportional to the inverse of channel matrix $\mathbf{H}$ as,

$$\mathbf{F} = \nu \mathbf{H}^{-1}. \tag{2.16}$$

If we assume that perfect CSIT is available, the ZFBF vectors are perfectly orthogonal to all the channel vectors. Then, multiuser interference is completely suppressed. Assuming that the transmit power is allocated uniformly as P/N_t, the SINR is,

$$\gamma_k = \frac{P}{N_t \sigma_k^2} |\mathbf{h_k}^H \mathbf{f}_k|^2 \tag{2.17}$$

In order to enhance performance of ZFBF, we can regularize the inverse of matrix. This vector perturbation linear precoding method that adds a multiple of identity matrix before inverting is known as Regularized Zero Forcing Beamforming (Negro et al., 2010). The Regularized ZFBF can be written as,

$$\mathbf{F} = \nu \mathbf{H}^H (\mathbf{H}\mathbf{H}^H + \beta \mathbf{I})^{-1} \tag{2.18}$$

where

$$\nu = \frac{1}{\sqrt{\mathrm{tr}\left(\mathbf{H}\mathbf{H}^H + \beta\mathbf{I}\right)^{-1}}} \tag{2.19}$$

The role of regularization is to reduce the effects of the largest eigenvalue. A suitable regularization factor β can maximize the SINR. In (Negro et al., 2010), optimum β is calculated as $\frac{K\sigma^2}{P}$.

2.3. Quantization of Channel State Information

The transmitter constructs the beamformer according to CSI. In practical communication systems, it is hard to acquire CSI of legitimate users perfectly, since the feedback channel is limited. In order to have CSIT, the receiver estimates and sends its CSI back to the transmitter. Sending full CSI back to transmitter increases feedback overhead. Infinite amount of bandwidth is required to send perfect CSI to transmitter. Thus, the sender is constrained to interpret available limited CSI. In order to achieve the goal of secure wireless communications, multiple antenna techniques and beamforming schemes with limited feedback is considered. This situation is the use of codebook that quantizes channel direction and/or channel quality information. In multiuser communications, different user's wireless channels fade independently. In order to maximize the secrecy sum capacity of multiple antenna downlink system, while achieving multiuser diversity, it is necessary to chose the best combination of active users.The channel quality information (CQI) is expressed as norm of channel vector, $\|\mathbf{h}_k\|$. With utilizing this information, transmitter can schedule users with more favorable channel conditions and discriminate the users with poor channel conditions. Due to the limited feedback, it may be necessary to quantize CQI with using codebook $\mathcal{V} = [v_1, \ldots, v_{2^Q}]$ where Q is the number of quantization bits. Transmitter interprets the quantized CQI and schedules users that maximize sum capacity. Also, the channel direction information (CDI) denoted as $\mathbf{g} = \mathbf{w}$, Equation (2.10).

Codebook based transmission schemes that the receiver sends back only index of the optimum beamformer by a few bits has commonly adopted in practice. The quantization of the channel direction information with vector quantization techniques was introduced by (Narula et al., 1998). Vector quantization maps a real or complex valued vector into a codebook. It is a lossy data compression and the codebook design should minimize the average distortion between original and quantized vectors. The design of codebook $C = [\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_N]$ for

multiple antennas can be stated as,

$$\mathbf{c}_{opt} = \min_{\mathbf{c}_i} \mathbb{E}\left[1 - |\mathbf{g}^H \mathbf{c}_i|^2\right],$$
$$\text{subject to } |\mathbf{c}_i^H \mathbf{c}_i| = 1 \;\; i = 1, \ldots, N.$$

where N is the size of codebook that is equal to 2^B and B is the number of quantization bits. The average SNR degradation can be written as (Jindal, 2006),

$$\gamma_d = \frac{\mathbb{E}\left[\|\mathbf{h}\|^2 - |\mathbf{h}^H \mathbf{c}_{opt}|^2\right]}{\mathbb{E}\left[\|\mathbf{h}\|^2\right]} = \mathbb{E}\left[1 - |\mathbf{g}^H \mathbf{c}_{opt}|^2\right] \tag{2.20}$$

that can be viewed as vector quantization problem with,

$$\begin{aligned} &\textbf{source input}: \quad \mathbf{g} \sim \text{uniform}\,(\mathcal{O}_{N_t}) \\ &\textbf{codebook}: \; C = [\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_N], \|\mathbf{c}_i\| = 1, \forall i \\ &\textbf{distortion metric}: \; d(\mathbf{g}, \mathbf{c}_i) = \sqrt{1 - |\mathbf{g}^H \mathbf{c}_{opt}|^2}, \; \forall \mathbf{g}, \forall i \end{aligned} \tag{2.21}$$

The Equation (2.21) is known as spherical vector quantization problem (Xia and Giannakis, 2006). The Lloyd algorithm was proposed to design such codebook design. (Love et al., 2003), (Mukkavilli et al., 2003), (Roh and Rao, 2006) showed that the codebook should be constructed by minimizing the maximum inner product of any two precoding vectors in the codebook. The Lloyd algorithm for vector quantization design is a iterative codebook improvement method. It can be described as follows (Allen Gersho, 1991);

- Given a codebook $C_m = [\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_N]$, find the optimal partition into quantization cells using the Nearest Neighbour Condition:

$$\mathcal{S}_i = \left\{\mathbf{g} : d(\mathbf{g}, \mathbf{c}_i) < d(\mathbf{g}, \mathbf{c}_j), \forall i \neq j\right\}. \tag{2.22}$$

- Using the Centroid Condition find the optimal reproduction of codebook $C_{m+1} = \{\text{Cent}(\mathcal{S}_i) : i = 1, \ldots, N\}$. The local correlation matrix for $\mathcal{S}_i$,

$$\Sigma_i = \frac{1}{\mathcal{S}_i} \sum_{\mathbf{h} \in \mathcal{S}_i} \mathbf{h}\mathbf{h}^H. \tag{2.23}$$

The Centroid Condition requires the maximizing the following,

$$\mathbf{c}_i^{opt} = \arg\max \mathbf{c}_i^H \Sigma_i \mathbf{c}_i. \tag{2.24}$$

In quantization process, each user chooses an codeword to quantize its CDI, $\mathbf{g}$, to an unit norm vector $\hat{\mathbf{h}}$ selected from a predetermined codebook size of 2^B. An optimal codeword to quantize its CDI is chosen according to following criterion,

$$i^* = arg \max_{1 \le i \le 2^B} \left| \mathbf{g}^H \mathbf{c}_i \right|. \tag{2.25}$$

Then, the quantized CDI $\hat{\mathbf{h}}$ is computed as $\mathbf{c}_{i^*}$. After selection of codebook index, the user feedbacks index i to transmitter in B bits. The quantization error arises because of limited feedback bits. In order to quantize CDI, Random Vector Quantization (RVQ) has been frequently used to analyse achievable rates. In RVQ, the N quantization vectors are independently chosen from the isotropic distribution on the N_t dimensional unit sphere. As the number of feedback bits B goes to infinity, RVQ becomes optimal. This feature of RVQ is useful for performance analysis (Yeung and Love, 2005). The expectation of this quantity over the channel realization $\mathbf{h}$ (Jindal, 2006) is given as,

$$\mathbb{E}\left[d^2(\mathbf{g}, \hat{\mathbf{h}})\right] = \mathbb{E}\left[\sin^2(\angle(\mathbf{g}, \hat{\mathbf{h}}))\right] \tag{2.26}$$

$$= \int_0^1 \left(1 - z^{N_t - 1}\right) 2^B dz \tag{2.27}$$

$$= \frac{1}{N_t - 1} \beta\left(2^B + 1, \frac{1}{N_t - 1}\right) \tag{2.28}$$

$$= 2^B \beta\left(2^B, \frac{N_t}{N_t - 1}\right) \tag{2.29}$$

where $\beta(.)$ is used to denote beta function that is defined in terms of gamma functions as $\beta(x, y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}$. The gamma function satisfies the fundamental properties $\Gamma(n) = (n-1)!$ and $\Gamma(x+1) = x\Gamma(x)$ and it is the extension of the factorial function to non-integers.

The expected quantization error is upper-bounded im Jindal (2006) and (Yeung and Love, 2005):

$$\mathbb{E}\left[d^2(\mathbf{g}, \hat{\mathbf{h}})\right] < 2^{\frac{-B}{N_t - 1}} \tag{2.30}$$

Since the quantization vectors are independent, it was shown that the cumulative distribution function of $\sin^2(\angle(\mathbf{g}, \hat{\mathbf{h}}))$ as,

$$Pr\left(\sin^2(\angle(\mathbf{g}, \hat{\mathbf{h}})) < z\right) = \left(1 - z^{N_t - 1}\right) 2^B. \tag{2.31}$$

For MISO point-to-point system, if the transmitter has perfect CSI optimum beamforming direction is along with channel vector $\mathbf{h}$. Then, corresponding ergodic capacity without secrecy concerns can be computed as,

$$C_{CSIT}(P) = \mathbb{E}\left[\log_2\left(1 + \frac{P\|\mathbf{h}\|^2}{\sigma^2}\right)\right]. \tag{2.32}$$

If transmitter has no CSIT and there is no secrecy concern, the optimum transmission strategy is to transmit independent and equal power signals from each of the N_t transmit antennas. The corresponding capacity is

$$C_{noCSIT}(P) = \mathbb{E}\left[\log_2\left(1 + \frac{P}{\sigma^2 N_t}\|\mathbf{h}\|^2\right)\right]. \tag{2.33}$$

Therefore, SNR loss is $10\log_{10}(N_t)$ in the case of no-CSIT. This SNR loss is reduced by providing partial CSI with RVQ. The corresponding capacity can be computed as (Jindal, 2006),

$$C_{RVQ}(P) = \mathbb{E}\left[\log_2\left(1 + \frac{P}{\sigma^2}\|\mathbf{h}\|^2\cos^2(\angle(\mathbf{g}, \hat{\mathbf{h}}))\right)\right] \tag{2.34}$$

$$\simeq \mathbb{E}\left[\log_2\left(1 + \frac{P}{\sigma^2}\|\mathbf{h}\|^2\left(1 - 2^{\frac{-B}{N_t-1}}\right)\right)\right] \tag{2.35}$$

The SNR loss compared to perfect CSI can be approximated as,

$$\Delta C_{RVQ} = 10\log_{10}\left(1 - 2^{\frac{-B}{N_t-1}}\right) \text{ dB}. \tag{2.36}$$

This section is devoted to provide a background for CSI quantization. The remainder of this section is organized as follows. In Section 2.3.1, the masked beamforming scheme that is discussed in Section 2.2.1.2 is considered with limited feedback link. In Section 2.3.2, the zero forcing beamforming method that is reviewed in Section 2.2.2.1 is considered with quantized CSIs at the transmitter. In Section 2.3.3, the quantization process of temporarily correlated fading channels via differential codebooks is provided.

2.3.1. Artificial Noise with Limited Feedback

The assumption of perfect CSI at transmitter is not valid in practice, since it requires infinite amount of bandwidth. The impairment caused by lack of perfect CSI with AN beamforming has been extensively studied in literature (Yang et al., 2012), (Zhang et al., 2015), (Wang et al., 2015), (Zheng and Wang, 2016), (Li et al., 2016). The imperfect CSI of legitimate user through limited feedback link causes an AN leakage which degrades the capacity

of legitimate user. Therefore, secrecy rate decreases under AN leakage (Lin et al., 2011). In the case of limited feedback, beamformer vectors are generated according to quantized CSIT. The quantized versions of precoding vectors $\mathbf{w}$ and $\mathbf{Q}$ are denoted as $\hat{\mathbf{w}}$ and $\hat{\mathbf{Q}}$ respectively. Due to the quantization errors, beamforming is not along with actual channel directions as depicted in Figure 2.4. Thus, the received signals at Bob and Eve can be written as,

$$\hat{y} = \mathbf{h}^H \hat{\mathbf{w}} s + \mathbf{h}^H \hat{\mathbf{Q}} \mathbf{a} + n, \tag{2.37}$$

$$\hat{y}_e = \mathbf{h}_e \hat{\mathbf{w}} s + \mathbf{h}_e \hat{\mathbf{Q}} \mathbf{a} + n_e, \tag{2.38}$$

the term $|\mathbf{h}^H \hat{\mathbf{Q}}|$ is not equal to zero. The angle between perfect and quantized CDIs can be expressed $\cos^2\theta = \cos^2(\angle(\mathbf{w}, \hat{\mathbf{w}})) = |\mathbf{w}^H \hat{\mathbf{w}}|^2$. Note that both $\mathbf{w}$ and $\hat{\mathbf{w}}$ are unit norm vectors.

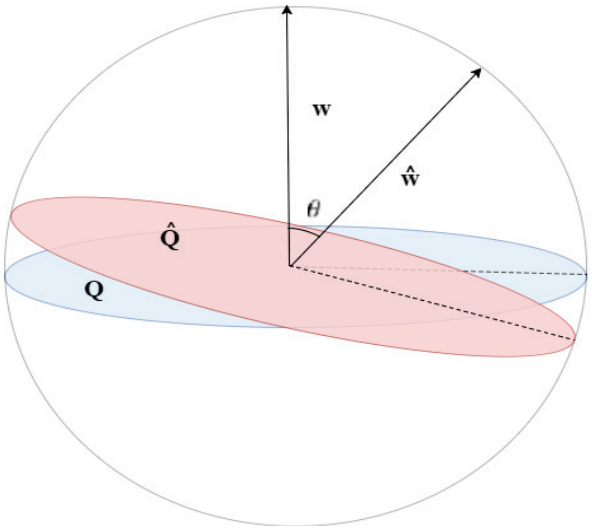

Figure 2.4. A geometric interpretation of quantized beamforming directions

The secrecy rate with AN beamforming for limited feedback link that causes a noise leakage is written as (Lin et al., 2011),

$$\hat{R}(\alpha) = \max\left(\mathbb{E}\{\log_2(1+\hat{\gamma}_b)\} - \mathbb{E}\{\log_2(1+\hat{\gamma}_e)\}\right)^+ \tag{2.39}$$

$$= \max\left(\mathbb{E}\left[\log_2\left(1 + \frac{\alpha P \|\mathbf{h}\|^2 \cos^2\theta}{\frac{(1-\alpha)P}{N_t-1}\|\mathbf{h}\|^2 \sin^2\theta + \sigma^2}\right)\right] - \mathbb{E}\left[\log_2\left(1 + \frac{\alpha P |\mathbf{h}_e \hat{\mathbf{w}}|^2}{\frac{(1-\alpha)P}{N_t-1}\|\mathbf{h}_e \hat{\mathbf{Q}}\|^2 + \sigma_e^2}\right)\right]\right)^+ \tag{2.40}$$

where $\|\mathbf{w}^H \hat{\mathbf{Q}}\|^2 = 1 - |\mathbf{w}^H \hat{\mathbf{w}}|^2 = \sin^2\theta$. It is worth to emphasize that as P goes to infinity,

secrecy rate converges to a constant.

$$\lim_{P\to\infty} \hat{R}(\alpha) = \left(\mathbb{E}\left[\log_2 \left(1 + \frac{\alpha \cos^2\theta}{\frac{(1-\alpha)}{N_t-1}\sin^2\theta + \sigma^2} \right) \right] - \mathbb{E}\left[\log_2 \left(1 + \frac{\alpha |\mathbf{h}_e \hat{\mathbf{w}}|^2}{\frac{(1-\alpha)}{N_t-1}||\mathbf{h}_e \hat{\mathbf{Q}}||^2 + \sigma_e^2} \right) \right] \right)^+ \tag{2.41}$$

As deduced from Equation (2.41), the rate of Bob and Eve remain constant as power goes to the infinity. In contrast, if perfect Bob CSIT is available, secrecy rate can be increased arbitrarily as power increases Lin et al. (2011).

$$\lim_{P\to\infty} R(\alpha) = \left(\mathbb{E}\left[\log_2 \left(1 + \frac{\alpha P |\mathbf{h}^H \mathbf{w}|^2}{\sigma^2} \right) \right] - \mathbb{E}\left[\log_2 \left(1 + \frac{\alpha |\mathbf{h}_e \mathbf{w}|^2}{\frac{(1-\alpha)}{N_t-1}||\mathbf{h}_e \mathbf{Q}||^2 + \sigma_e^2} \right) \right] \right)^+ \tag{2.42}$$

The Equation (2.42) implies that as P goes to the infinity, first term also goes to infinity where second term remain constant. In addition to quantization errors, channel estimation errors also one of the reason of imperfect CSIT. This specific problem is addressed in (Peng et al., 2014), (Wang et al., 2015).

2.3.2. Zero Forcing Beamforming with Limited Feedback

In the case of partial CSI, multi-user interference can not be eliminated completely. In multi-user networks, each user chooses an codeword to quantize its CDI $\mathbf{g}_k = \frac{\mathbf{h}_k}{||\mathbf{h}_k||}$ to an unit norm vector $\hat{\mathbf{g}}_k$ selected from a predetermined codebook. The RVQ codebook C_k is adopted where $C_k = \left\{ \mathbf{c}_{k_1}, \mathbf{c}_{k_2}, ..., \ldots, \mathbf{c}_{k_i}, \ldots, \mathbf{c}_{k_{2B}} \right\}$ for each user. An optimal codeword to quantize its CDI is chosen according to following criterion,

$$k_{i^*} = \arg \max_{1\le i\le 2^B} \left| \mathbf{g}_k^H \mathbf{c}_{k_i} \right|. \tag{2.43}$$

After selection of codebook index, each Bob feds back its CDI to Alice in B bits. Quantization error arises because of limited feedback link. The relation between perfect CDI $\mathbf{g}_k$ and codeword $\hat{\mathbf{g}}_\mathbf{k} = \mathbf{c}_{\mathbf{k}_{i^*}}$ is given as,

$$\mathbf{g}_k = \hat{\mathbf{g}}_\mathbf{k} \cos\theta_\mathbf{k} + \mathbf{g}_\mathbf{k}^\perp \sin\theta_\mathbf{k}, \tag{2.44}$$

where $\mathbf{g}_\perp^k$ is a unit norm vector orthogonal to $\hat{\mathbf{g}}_\mathbf{k}$, $\theta_k = \angle(\mathbf{g}_k, \hat{\mathbf{g}}_\mathbf{k})$ and the quantization error follows $\frac{N_t-1}{N_t}\delta \le E\{\sin\theta_k\} \le 2^{\frac{-B}{N_t-1}}$, Jindal (2006). The selected quantized vectors are fed back

to transmitter with quantized CDI matrix $\hat{\mathbf{H}} = [\hat{\mathbf{g}}_1, \ldots, \hat{\mathbf{g}}_k, \ldots, \hat{\mathbf{g}}_K]^H$ which is the quantized version of the joint channel matrix $\mathbf{H}$. Thus, SINR at k^{th} user can be expressed as,

$$\gamma_k = \frac{\frac{P}{N_t}|\mathbf{h_k}^H \hat{\mathbf{f}}_k|^2}{\frac{P}{N_t}\sum_{j=1, j\neq k}^{N_t}|\mathbf{h_k}^H \hat{\mathbf{f}}_j|^2 + \sigma_k^2} \tag{2.45}$$

where $[\hat{\mathbf{f}}_1, \ldots, \hat{\mathbf{f}}_k, \ldots, \hat{\mathbf{f}}_K]$ quantized versions of $\mathbf{f}_k$ and it is constructed as $\hat{\mathbf{F}} = \hat{\mathbf{H}}^H \left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H\right)^{-1}$. The SNR loss due to the imperfect CSIT while employing ZFBF is computed using Jensen inequality as (Jindal, 2006),

$$\Delta R \leq \log_2\left(1 + \frac{P}{\sigma_k^2 N_t}(N_t - 1)\,\mathbb{E}\left[\|\mathbf{h}_k\|^2\right]\mathbf{E}\left[|\mathbf{g_k}^H \hat{\mathbf{f}}_j|^2\right]\right) \tag{2.46}$$

$$\leq \log_2\left(1 + \frac{P}{\sigma_k^2 N_t}\mathbb{E}\left[d^2(\mathbf{g_k}, \hat{\mathbf{f}}_k)\right]\right) \tag{2.47}$$

$$< \log_2\left(1 + \frac{P}{\sigma_k^2 N_t} 2^{\frac{-B}{N_t - 1}}\right). \tag{2.48}$$

Also, in order to keep a rate offset no larger than $\log_2 c$(per user) between zero-forcing with perfect CSI and with imperfect CSI, the number of sufficient bits are calculated as (Jindal, 2006),

$$B \simeq \frac{N_t - 1}{3} P_{\text{dB}} - (N_t - 1)\log_2(c - 1) \tag{2.49}$$

If the SNR is low, limited feedback ZFBF scheme performs nearly same as perfect CSI. However, as SNR increases gap between perfect CSI ZFBF and required feedback bits increases.

2.3.3. Differential Codebook Design

In fading channels, the channel variations are defined as the Gauss-Markov process for modeling the time correlation;

$$\mathbf{h}_\tau = z\mathbf{h}_{\tau-1} + \sqrt{1 - z^2}a_\tau. \tag{2.50}$$

where the a_τ is complex normal Gaussian distributed innovation process. The z is time correlation parameter ($0 \leq z \leq 1$), and it is the measure of correlation between successive time instants. If z has a large value, this means that the correlation of vector $\mathbf{h}_{\tau-1}$ and vector $\mathbf{h}_\tau$ is high. Since the channels do not experience a sudden severe fading in that case.

The differential codebook is generated as follows (Choi et al., 2012);

- $\tau = 0$:

  The channel information in the first time slot is quantized according to the minimum distance criterion using the initial random vector quantizer codebook.

$$i^* = \arg \min_{1 \leq i \leq 2^B} |1 - \mathbf{g}_0{}^H \mathbf{c}_i|. \tag{2.51}$$

  The $\mathbf{g}_0 = \frac{h_0}{\|h_0\|}$ is the normalized version of CDI ($\mathbf{h}_\tau$) at $\tau = 0$. Then, beamforming vector can be computed by using the minimum distance criteria,

$$\mathbf{w}_0 = \mathbf{c}_{i^*}. \tag{2.52}$$

where $\mathbf{w}_\tau$ is the beamforming vector and $\mathbf{w}_0$ is the beamforming vector at time $\tau = 0$.

- For $\tau = 1, 2, ...\tau_{max}$:

  The predetermined polar-cap differential codebook is used. To construct the basis polar-cap differential codebook $\tilde{C}^\tau$,

$$\tilde{C}^\tau = \left\{ \tilde{\mathbf{c}}_{1,\tau}, \begin{bmatrix} \sqrt{1-\delta_\tau^2} \\ \delta_\tau \xi_{\mathbf{2}} \end{bmatrix}, \ldots, \begin{bmatrix} \sqrt{1-\delta_\tau^2} \\ \delta_\tau \xi_{\mathbf{2^B}} \end{bmatrix} \right\}, \tag{2.53}$$

  form is used. The $\tilde{\mathbf{c}}_{1,\tau}$ can be any unit vector. For simplicity, it is chosen as $\tilde{\mathbf{c}}_{1,\tau} = [1, 0, \ldots, 0]^T$ in this study. The δ_τ, which specifies the polar container size, significantly affects system performance. This parameter can be set to adaptive or fixed. By selecting $\tilde{\mathbf{c}}_{1,\tau}$ and δ_τ, codewords placed around the polar-cap can be generated. Also, the $\{\xi_{\mathbf{2}}, \xi_{\mathbf{3}}, \ldots, \xi_{2^B}\}$ is generated as complex Grassmannian Line Packets where $\xi_i \in C^{(N_t-1)\times 1}$. The reason for using Grassmannian line packing here is that it provides good performance for Rayleigh fading channels. Once the polar cap codebook is created, it can be used repeatedly for different τ instants. After the codebook is determined, the user and the transmitter compute the $\tilde{\mathbf{c}}_{1,\tau}$ vector via using the quantized channel direction vector $\hat{\mathbf{h}}_{\tau-1}$ constructs a rotation matrix, $\mathbf{R}_{\hat{h}_{\tau-1}}$.

  Rotation function can be defined as follows,

$$\mathbf{r} : \mathcal{B}_{\delta_\tau}(\tilde{\mathbf{c}}_{1,\tau}) \mapsto \mathcal{B}_{\delta_\tau}(\hat{\mathbf{h}}_{\tau-1}), \tag{2.54}$$

$$\hat{\mathbf{h}}_{\tau-1} = \mathbf{r}(\hat{\mathbf{h}}_{\tau-1})\tilde{\mathbf{c}}_{1,\tau}, \tag{2.55}$$

$$= \mathbf{R}_{\hat{h}_{\tau-1}} \tilde{\mathbf{c}}_{1,\tau}. \tag{2.56}$$

Householder transformation is used to construct the rotation matrix:

$$\mathbf{v} = \tilde{\mathbf{c}}_{1,\tau} - \hat{\mathbf{h}}_{\tau-1}, \tag{2.57}$$

$$\mathbf{R}_{\hat{h}_{\tau-1}} = \mathbf{I} - \frac{\mathbf{v}\mathbf{v}^{\dagger}}{\mathbf{v}^{\dagger}\tilde{\mathbf{w}}_{1,\tau}}. \tag{2.58}$$

After the rotation matrix is obtained by using Householder transformation as above, the entire basis polar-cap codebook is rotated with the rotation matrix.

$$C^{\tau} = \left\{ \mathbf{R}_{\hat{h}_{\tau-1}} \tilde{\mathbf{c}}_{j,\tau}; \quad j = 1, 2, ..., 2^{B} \right\}. \tag{2.59}$$

The new codebook, which has been rotated by multiplying each column rotation matrix of the basis polar codebook is generated as, $C^{\tau} = \{\mathbf{c}_{1,\tau}, \mathbf{c}_{2,\tau}, \ldots, \mathbf{c}_{2^{B},\tau}\}$.

The channel information of the user at time instant τ is quantized by this codebook and sent to transmitter. The transmitter utilizes this information as the beamforming vector $\mathbf{w}_{\tau}$.

$$i^{*} = \arg \min_{1<i<2^{B}} |1 - \mathbf{g}_{\tau}{}^{H} \mathbf{c}_{i,\tau}|, \tag{2.60}$$

$$\mathbf{w}_{\tau} = \mathbf{c}_{i^{*},\tau}. \tag{2.61}$$

- $\tau = \tau_{max} + 1$:
  Processes are reset at a later then the specified τ_{max} period. The duration of τ_{max} can be chosen as coherence time.

CHAPTER 3

SECURE SINGLE USER MULTIPLE INPUT SINGLE OUTPUT SYSTEMS

In this chapter, two different secure MISO system models with different channel conditions are studied. In both model, the problem of physical layer security is considered under limited CSI (quantized) feedback link. The first system model is the single user MISO system operating under quasi-static Rayleigh fading channels (Ozdogan et al., 2016), (Ozbek et al., 2017). The wireless channel is constant for a block of transmission and it varies independently and randomly between blocks. In the second system model, we investigate the problem of secure single user MISO systems over temporally correlated channels (Ozdogan et al., 2017a). The channel at successive time instants are correlated and this characteristic of wireless channels is utilized to achieve secure communications.

3.1. System Model for Block Fading Channels

Consider a multiuser MISO downlink system operating under secrecy constraint. The wireless system consists of one base station (Alice) with N_t antennas, K active legitimate users where each one has single antenna and N_e cooperating single antenna eavesdroppers. The N_e cooperating passive single antenna eavesdroppers that are dispersed geographically can correspond to one eavesdropper with N_e antennas. The aim of Alice is to send confidential messages to one intended legitimate user. In order to increase secrecy capacity, the best Bob which has the highest channel gain is selected from the set of active K users.

Since the eavesdroppers overhear the secret messages illegally, the message signal is masked with AN to disrupt the reception of eavesdroppers while guaranteeing secrecy. We assume that CSI of legitimate users is perfectly estimated at receiver side. Moreover, we assume that Alice may acquire the perfect or the quantized CSI of legitimate users depending on the considered scenario. However, eavesdroppers are passive and they do not reveal their location. Therefore, the transmitter has no knowledge regarding to CSI of Eve, which is highly probable scenario in practical cases.

The transmitted signal vector $\mathbf{x}_k$ constructed under AN beamforming is expressed as,

$$\mathbf{x}_k = \mathbf{w}_k s_k + \mathbf{Q_k a_k} \tag{3.1}$$

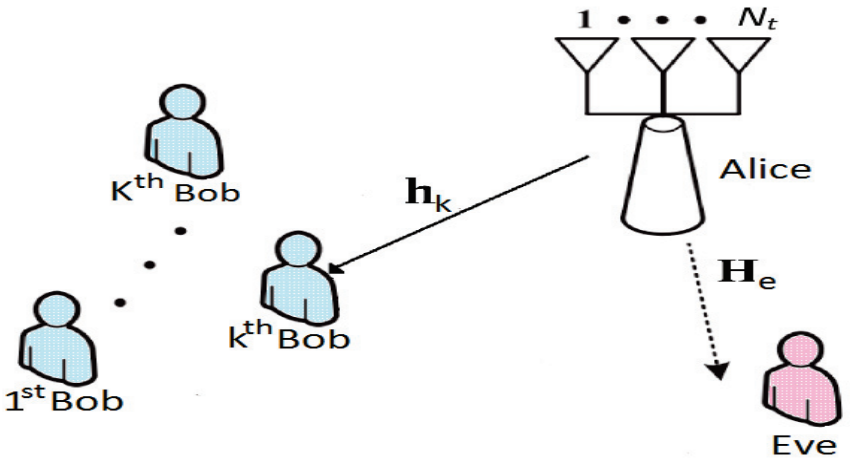

Figure 3.1. A system model that consists a multi-antenna transmitter, K legitimate receivers with single antenna and an eavesdropper with multiple-antenna

where s_k is the information-bearing signal with power $\mathbb{E}[\{|s_k|^2\}] \leq P_s$ and $\mathbf{w} \in C^{N_t \times 1}$ is the precoding vector at Alice. Also, $\mathbf{a}_k = [a_1, a_2, \ldots, a_{N_t-1}]^T \in \mathbb{C}^{N_t-1 \times 1}$ is the AN which is a random Gaussian vector with power $E[\{\|\mathbf{a}_k\|^2\}] \leq P_a$ and $\mathbf{Q}_k \in \mathbb{C}^{N_t \times N_t-1}$ is the AN beamformer with orthonormal columns that form the AN subspace. The beamformers $\mathbf{w}_k$ and $\mathbf{Q}_k$ are determined through available CSI at Alice. P is the total transmit power which is equal to sum of power of information and AN signal, where $P_s = \alpha P$ and $P_a = \frac{1-\alpha}{N_t-1} P$ where α is power allocation parameter and its value changes between 0 and 1. As α increases, the power allocated for information signal increases and the power of AN signal decreases. This power apportionment between information and AN signals affects the secrecy capacity. According to availability of CSI of legitimate user at Alice (perfect or quantized), the α parameter should be chosen to provide an optimum secrecy capacity.

The received signals at the Bob and the Eve are respectively,

$$y_k = \mathbf{h}_k^H \mathbf{w}_k s_k + \mathbf{h}_k^H \mathbf{Q}_k \mathbf{a}_k + n_k \tag{3.2}$$

$$\mathbf{y}_e = \mathbf{H}_e \mathbf{w}_k s_k + \mathbf{H}_e \mathbf{Q}_k \mathbf{a}_k + \mathbf{n}_e \tag{3.3}$$

where the channel vector of kth legitimate user is $\mathbf{h}_k \in C^{N_t \times 1}$, the channel matrix of eavesdropper is denoted by $\mathbf{H}_e \in C^{N_e \times N_t}$, n_k is the complex AWGN modelled by $C\mathcal{N}(0, \sigma^2)$ and each element of $\mathbf{n}_e$ represents complex AWGN for Eve side with zero mean and variance σ_e^2.

For perfect CSIT, the precoding vector is determined by $\mathbf{w}_k = \mathbf{g}_k$ and $\mathbf{Q}_k$ whose columns form an orthonormal basis for the null space of $\mathbf{g}_k$ defined by $\|\mathbf{g}_k^H \mathbf{Q}_k\| = 0_{1 \times N_t}$. The secrecy capacity (i.e. the maximum transmission rate at which the eavesdropper is unable to

decode any information) is equal to the difference between the two channel capacities. Consequently, confidential communication is not possible unless Bob's channel has a better SNR than eavesdropper's channel.

Then, the achievable secrecy capacity with perfect CSI at Alice is given by,

$$R = \max \left\{ \mathbb{E} \left\{ \log_2 \left(1 + \gamma_k \right) \right\} - \mathbb{E} \left\{ \log_2 \left| \mathbf{I} + \gamma_e \right| \right\} \right\}^+ \tag{3.4}$$

where γ_k and γ_e which denote the instantaneous SNRs belonging to the selected Bob and Eve, respectively are defined as in (Li et al., 2016),

$$\gamma_k = \alpha \rho \left\| \mathbf{h}_k \right\|^2 \tag{3.5}$$

where $\rho = \frac{P}{\sigma^2}$ is the average SNR at each legitimate user.

$$\gamma_e = \alpha (\mathbf{H}_e \mathbf{g}_k)(\mathbf{H}_e \mathbf{g}_k)^H \left(\frac{(1-\alpha)}{N_t - 1} (\mathbf{H}_e \mathbf{Q}_k)(\mathbf{H}_e \mathbf{Q}_k)^H \right)^{-1} \tag{3.6}$$

Therefore, we consider the worst case in terms of secrecy capacity.

3.1.1. Threshold based selection at legitimate user side

In secure multiuser systems, the intended user can be scheduled according to most favourable channel conditions to increase secrecy capacity. The transmitter selects this user through available CSI at Alice. Generally, only quantized CSI is available at Alice due to the capacity limitations on the feedback channel. As the number of active users K grows, the feedback load increases in multiuser multiantenna sytems. In order to reduce this feedback load while achieving the same secrecy capacity, we apply a threshold at legitimate user side to discriminate users with poor channel conditions. Accordingly, the legitimate users having a low norm should not take part in the user selection algorithm, nor requires to fed back their CSI. Thus, only legitimate users above this threshold send their CSI to Alice.

The threshold based selection namely $\mathcal{T}_1$ criterion applies a threshold, γ_{th}, and constructs a set $\mathcal{U}_1$ by selecting users that satisfy the following threshold condition (Gesbert and Alouini, 2004). Via this threshold, users with poor channel conditions are discriminated at the user side.

$$\mathcal{U}_1 = \left\{ k \in K : \left\| \mathbf{h}_k \right\|^2 > \gamma_{th} \right\} \tag{3.7}$$

The threshold value can be obtained either analytically or by simulation in order to guarantee an average number of users $\bar{K}$ that fed back their instantaneous CSI to the base

station.

$$\bar{K} = KPr\{k \in \mathcal{U}_1\} = KPr\left\{||\mathbf{h}_k||^2 > \gamma_{th}\right\} \tag{3.8}$$

The set $\mathcal{U}_1$ is determined by the incomplete gamma distribution $\Gamma(N_t, 1)$ which can be bounded by (Sharif and Hassibi, 2005), (Zhang et al., 2008)

$$[1 - \exp(-\beta\gamma_{th}))]^{N_t} \leq \int_0^{\gamma_{th}} f_\gamma(\gamma)d\gamma \leq [1 - exp(-\gamma_{th}))]^{N_t} \tag{3.9}$$

where $\beta = (N_t!)^{\frac{-1}{N_t}}$ and $f_\gamma(\gamma)$ is the probability density function with $\chi^2_2(N_t)$. Then, we can obtain:

$$Pr\{k \in \mathcal{U}_1\} = \sum_{b=0}^{N_t-1} \frac{\exp(-\gamma_{th})(\gamma_{th})^b}{b!} \tag{3.10}$$

Thus, the average number of users that feedback their CSI to Alice can be determined by,

$$\bar{K} = K \sum_{b=0}^{N_t-1} \frac{\exp(-\gamma_{th})(\gamma_{th})^b}{b!} \tag{3.11}$$

After $\mathcal{T}_1$ criterion is applied at legitimate user side, $\bar{K}$ users feedback their CDI to the base station and their CQI is assumed to be perfectly available at the Alice. Then, the intended legitimate user is selected at the Alice as,

$$k = \arg\max_{j \in \mathcal{U}_1} \left\|\mathbf{h}_j\right\|^2 \tag{3.12}$$

3.1.2. Secrecy capacity with quantized feedback link

Each user that satisfies $\mathcal{T}_1$ criterion chooses an codeword to quantize its CDI $\mathbf{g}_k$ to an unit norm vector $\hat{\mathbf{g}}_k$ selected from a predetermined codebook as described in Section 2.3.2. In the case of quantized CDI, transmitted signal can be denoted as,

$$\mathbf{x}_k = \hat{\mathbf{g}}_k s_k + \hat{\mathbf{Q}}_k \mathbf{a}_k, \tag{3.13}$$

where $\hat{\mathbf{Q}}_k$ and $\hat{\mathbf{g}}_k$ are quantized version of $\mathbf{Q}_k$ and $\mathbf{g}_k$. Then, the received signals at the legitimate receiver and eavesdropper can be written as

$$y_k = ||\mathbf{h}_k||(\mathbf{g}_k{}^H \hat{\mathbf{g}}_k)s_k + ||\mathbf{h}_k||(\mathbf{g}_k{}^H \hat{\mathbf{Q}}_k)\mathbf{a}_k + n_k, \tag{3.14}$$

$$\mathbf{y}_e = \mathbf{H}_e \hat{\mathbf{g}}_k s_k + \mathbf{H}_e \hat{\mathbf{Q}}_k \mathbf{a}_k + \mathbf{n}_e, \tag{3.15}$$

In the case of quantized CSI, the SINRs at k^{th} Bob can be expressed by,

$$\hat{\gamma_k} = \frac{\alpha ||\mathbf{h}_k||^2 |\mathbf{g}_k{}^H \hat{\mathbf{g}}_k|^2}{\frac{1-\alpha}{N_t-1} ||\mathbf{h}_k||^2 ||\mathbf{g}_k{}^H \hat{\mathbf{Q}}_k||^2 + \frac{1}{\gamma}}, \tag{3.16}$$

The measure of how quantized CDI align with exact CDI can be denoted by $\cos^2\theta_k = |\mathbf{g}_k{}^H \hat{\mathbf{g}}_k|^2$ and $\sin^2\theta_k = |\mathbf{g}_k{}^H \hat{\mathbf{Q}}_k|^2$ as described in Equation 2.40. Also, the relation can be written as, $|\mathbf{g}_k{}^H \hat{\mathbf{g}}_k|^2 + |\mathbf{g}_k{}^H \hat{\mathbf{Q}}_k|^2 = 1$ as described in Section 2.3.1. The SINR of legitimate user can be written as (Lin et al., 2011),

$$\hat{\gamma_k} = \frac{\alpha ||\mathbf{h}_k||^2 \cos\theta_k^2}{\frac{1-\alpha}{N_t-1} ||\mathbf{h}_k||^2 \sin\theta_k^2 + \frac{1}{\rho}} \tag{3.17}$$

In the case of quantized CSI, the SINRs at Eve can be written by,

$$\hat{\gamma_e} = \alpha (\mathbf{H}_e \hat{\mathbf{g}}_k)(\mathbf{H}_e \hat{\mathbf{g}}_k)^H \left(\frac{1-\alpha}{N_t - 1} (\mathbf{H}_e \hat{\mathbf{Q}}_k)(\mathbf{H}_e \hat{\mathbf{Q}}_k)^H \right)^{-1} \tag{3.18}$$

Thus, secrecy capacity with quantized CSIT is

$$R^q = \max \left\{ \mathbb{E}\left\{ \log_2 (1 + \hat{\gamma_k}) \right\} - \mathbb{E}\left\{ \log_2 |\mathbf{I} + \hat{\gamma_e}| \right\}, 0 \right\}^+ \tag{3.19}$$

In contrast to case that Alice has perfect CSI of legitimate user, the limited CDI causes an artificial noise leakage. The noise that leaks from intended user's null space, $||\mathbf{h}_k||^2 |\mathbf{g}_k{}^H \hat{\mathbf{Q}}_k|^2$, decreases the secrecy capacity. Even γ goes to infinity, secrecy capacity converges to a constant value as defined in Equation 3.17 .

3.1.3. The Case of Known Eavesdropper's CSI at transmitter

We also consider the same system model given in Section 3.1 by focusing only on the case that Alice has knowledge of CSI of Eve. In contrast to the case that eavesdropper is hidden and CSI of Eve at Alice is not available, we assume that eavesdropper is somehow detected and its CSI is obtained. This may not be the case in practice since they are passive in general. Nevertheless, we examine the impact of quantized and perfect CSI of Eve at Alice on the secrecy capacity and compare its performance with AN assisted beamforming.

Firstly, $\mathcal{T}_1$ is applied at legitimate user side as in Section 3.1 and only CSI of $\bar{K}$ active user is fed back to Alice. Among these $\bar{K}$ legitimate users, Bob with most favourable condition (greatest norm) is selected at Alice for secure communication. Then, the transmitted signal is

formed based on GSVD (Khisti and Wornell, 2010) and the received signals at Bob and Eve are given respectively by,

$$y_k = \mathbf{h}_k^H \mathbf{x}_k + n_k \tag{3.20}$$

$$\mathbf{y}_e = \mathbf{H}_e \mathbf{x}_k + \mathbf{n}_e \tag{3.21}$$

where $\mathbf{x}_k$ is the transmitted signal vector of k^{th} user along direction Ψ_{max}

$$\mathbf{x}_k = \Psi_{max} s_k. \tag{3.22}$$

Secrecy capacity of system with available CSI of Eve at Alice can be computed as given in (Khisti and Wornell, 2010) as described in Section 2.2.1.1:

$$R^p = \left\{ \log \lambda_{\max} \left(\mathbf{I} + P\mathbf{h}_k \mathbf{h}_k^H, \mathbf{I} + P\mathbf{H}_e^H \mathbf{H}_e \right) \right\}^+ \tag{3.23}$$

where $\lambda_{\max}$ denotes the largest generalized eigenvalue of its argument pair and it is the maximum of the Rayleigh quotient.

3.1.4. Performance Evaluations

In this section, we present simulation results by setting the number of transmitter antennas as $N_t = 4$ at Alice. Threshold values of T_1 criterion is analytically adjusted to get average number of users that feedback their CSI to transmitter as $\bar{K} = 4$. If the number of active legitimate users is given by $K = [10, 20, 30, 40, 50]$, their corresponding threshold values are determined as $\gamma_{th} = [4.15, 5.5, 6.2, 6.67, 7.0]$. According to these threshold values, the set $\mathcal{U}_1$ is constructed and legitimate users in this set fed back their CSI to the Alice in B bits.

The figures from Figure 3.2 to Figure 3.7 show the optimal power allocation parameters for different quantization bits and SNR values when ECSIT is not available at transmitter. In these figures, full feedback (FF) refers to case that all users feds back their CSI to Alice and T1 criterion considering different number of feedback bits. As expected, a higher number of quantization bits results in greater secrecy rates. When CSI of Eve is not available at Alice, a portion of the power should be dedicated for AN to interrupt reception of Eve. The optimal power allocation parameter α depends on the CSI quality of legitimate users. If the feedback bits are sufficiently large, the optimal value is calculated by $\alpha = \frac{\sqrt{1}}{\sqrt{1}+\sqrt{Ne}}$ (Li et al., 2016). For example, $\alpha = 0.414$ for $N_e = 2$. However, as the number of quantization bits reduces, less

power should be allocated to AN signal in order to prevent severe AN leakage such that α approximates 1.

In Figure 3.8 and Figure 3.9, the impact of the number of antennas at Eve are analyzed by determining the optimal α values to maximize secrecy capacity. In Figure 3.8, the CSI of legitimate user is perfectly available at transmitter. In figure 3.9, the number of quantization bits $B = 12$. As observed from the results, when a perfect CSI of legitimate user is available at Alice, secrecy capacity is not bounded and can be increased with SNR for $N_t \geq N_e + 1$.

In Figure 3.10 and Figure 3.11, the impact of the number of antennas at Eve are examined when CSI of Eve is known at transmitter. In Figure 3.10, the CSIs of legitimate user and eavesdropper are perfectly available at transmitter. In Figure 3.11, quantized versions of these CSIs are available at Alice($B = 12$). In the case that we have only quantized CSIs, achievable secrecy more vulnerable to eavesdropper with high number of antennas.

In Figure 3.12, Figure 3.13 and Figure 3.14, we compare secrecy capacity results for the case of CSI of Eve is available at the Alice (known ECSIT) and is not available at the Alice (unknown ECSIT) by employing full feedback and T1 criterion through limited feedback link. When CSI of legitimate users and eavesdropper are perfectly known at Alice, the eavesdropper is not allowed to infer any information. However, the feedback channel is limited and only quantized CSI of Bob and Eve may be available at the Alice in practical systems. When the quantized CSI of Eve and Bob are available at the Alice, the secrecy capacity is lower than the case of unknown CSI of Eve. The case of the quantized CSI of Bob and unknown CSI of Eve at Alice provides a considerable gain on secrecy capacity depending on the number of quantization bits and the number of active legitimate users. More specifically, in Figure 3.12 and Figure 3.13, we compare the cases known ECSIT and unknown ECSIT according to their multiuser diversity performance. In Figure 3.14, the cases known ECSIT and unknown ECSIT are compared in the aspect of SNR.

In Figure 3.15, the secrecy capacity for different number of quantization bits for CSI of Bob is illustrated for CSI of Eve is available at the Alice through limited feedback link. According to the results, an increment in SNR causes a loss in secrecy capacity since the eavesdropper has more antenna than intended user and beamforming is no longer in optimal direction. This situation is in sharp contrast to that with perfect CSI.

In Figure 3.16, the secrecy capacity for different number of quantization bits for CSI of Bob is illustrated for CSI of Eve is unknown at Alice. When the number of quantization bits are increased, the gain is increased since the leakage to Eve is also reduced. It shows that if number of quantization bits is adequate, it is possible to provide secrecy gain with SNR increment.

For $B = 12$ and $K = 50$, the total feedback load is $50 \times 12 = 600$ bits per channel use for full feedback case . If T_1 criterion is employed, only 4 users on average fed back their

CSI to the Alice and total feedback load reduces to $4 \times 12 = 48$ bits. It is also observed that T_1 criterion does not causes a secrecy capacity degradation compared to full feedback case while providing reduction on feedback load which varies between $60\% - 92\%$ depending on the average number users K.

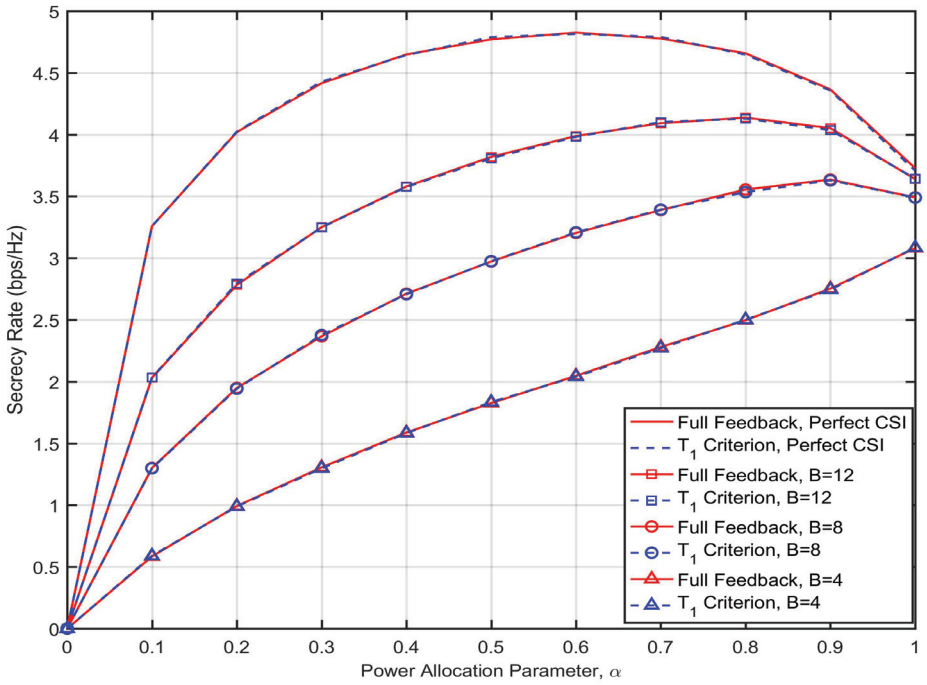

Figure 3.2. Secrecy rate versus α for different number of quantization bits in the case that CSI of Eve is unknown at Alice and $N_e = 1$, SNR= 10 dB, $K = 50$.

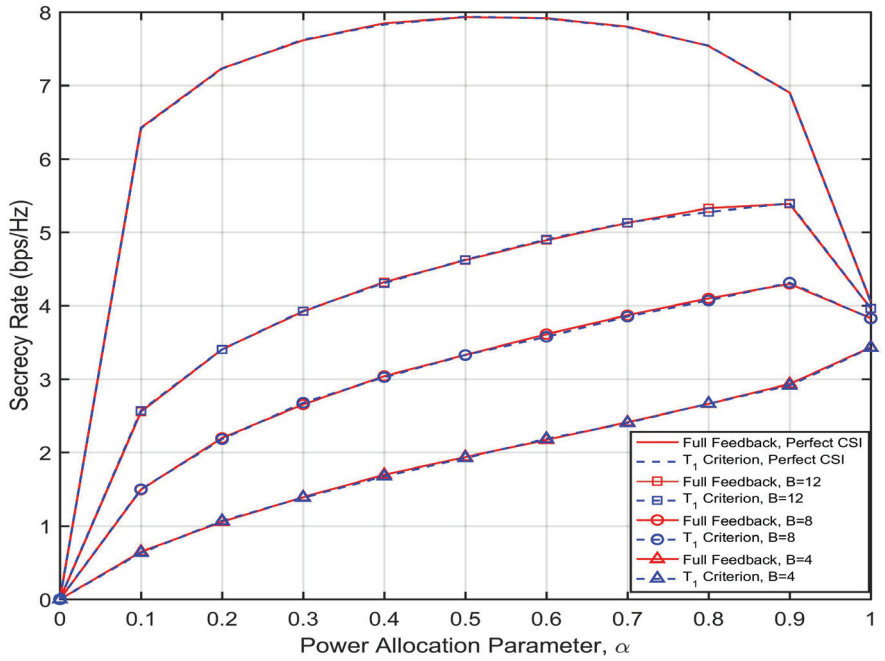

Figure 3.3. Secrecy rate versus α for different number of quantization bits in the case that CSI of Eve is unknown at Alice and $N_e = 1$, SNR= 20 dB, $K = 50$.

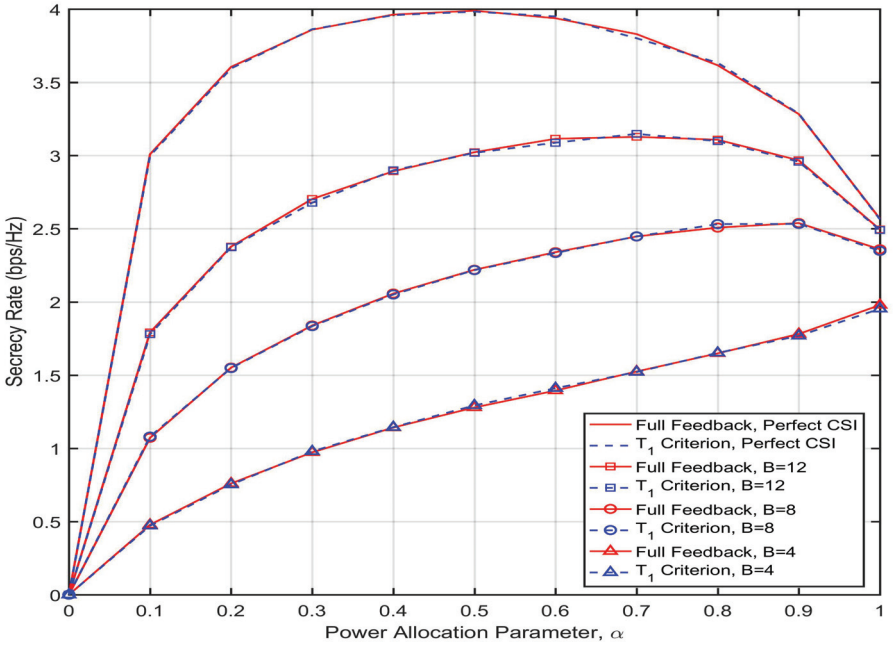

Figure 3.4. Secrecy rate versus α for different number of quantization bits in the case that CSI of Eve is unknown at Alice and $N_e = 2$, SNR= 10 dB, $K = 50$.

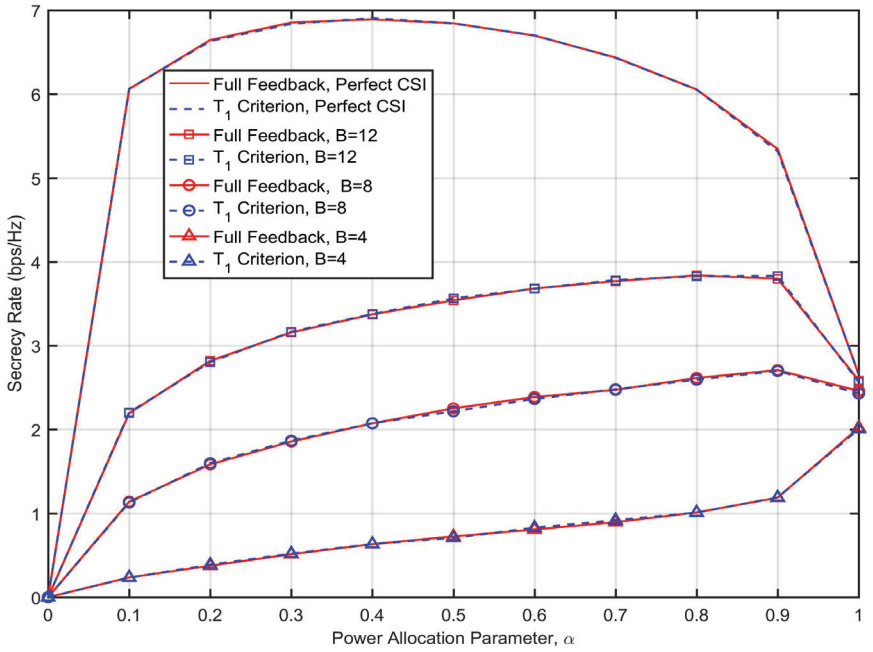

Figure 3.5. Secrecy rate versus α for different number of quantization bits in the case that CSI of Eve is unknown at Alice and $N_e = 2$, SNR= 20 dB, $K = 50$.

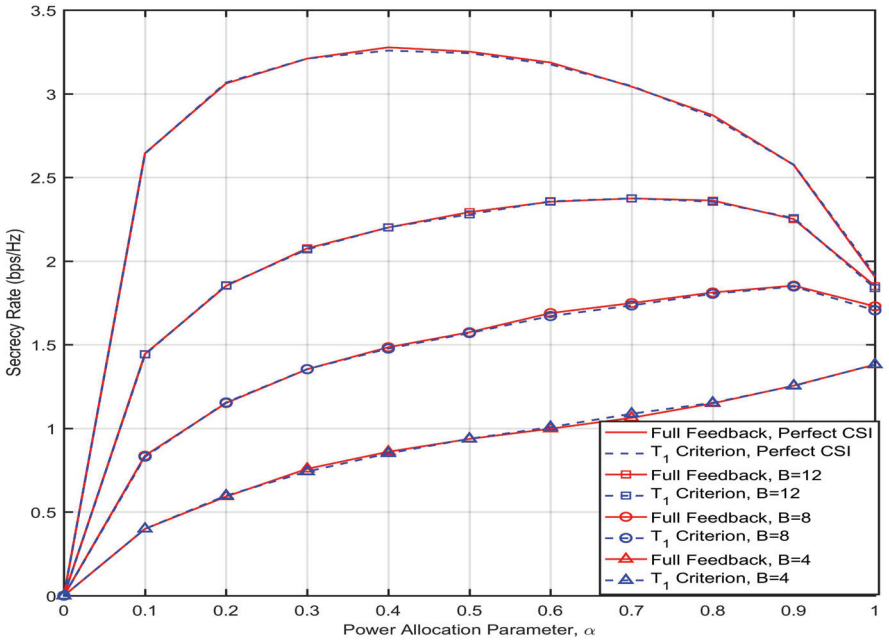

Figure 3.6. Secrecy rate versus α for different number of quantization bits in the case that CSI of Eve is unknown at Alice and $N_e = 3$, SNR= 10 dB, $K = 50$.

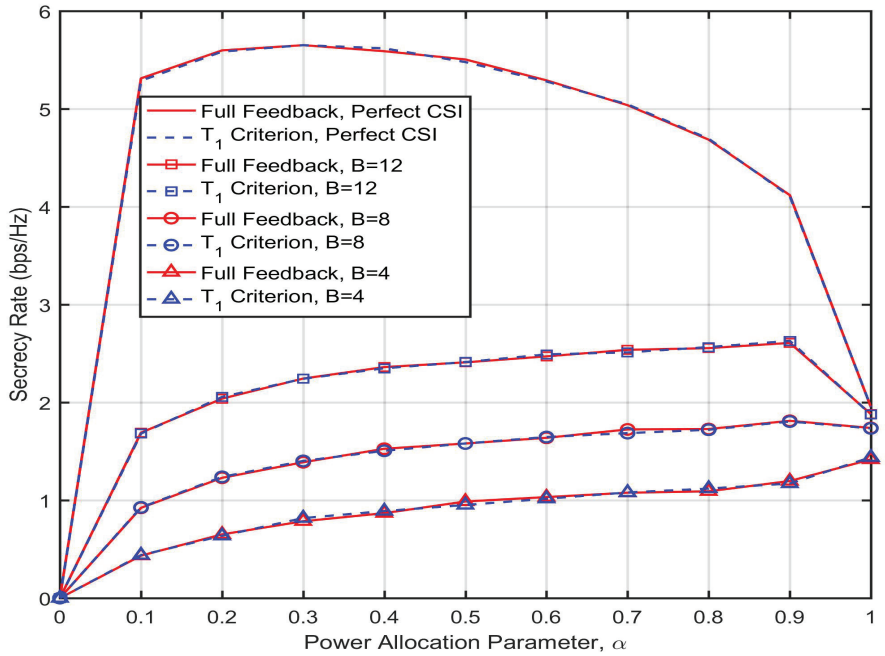

Figure 3.7. Secrecy rate versus α for different number of quantization bits in the case that CSI of Eve is unknown at Alice and $N_e = 3$, SNR= 20 dB, $K = 50$.

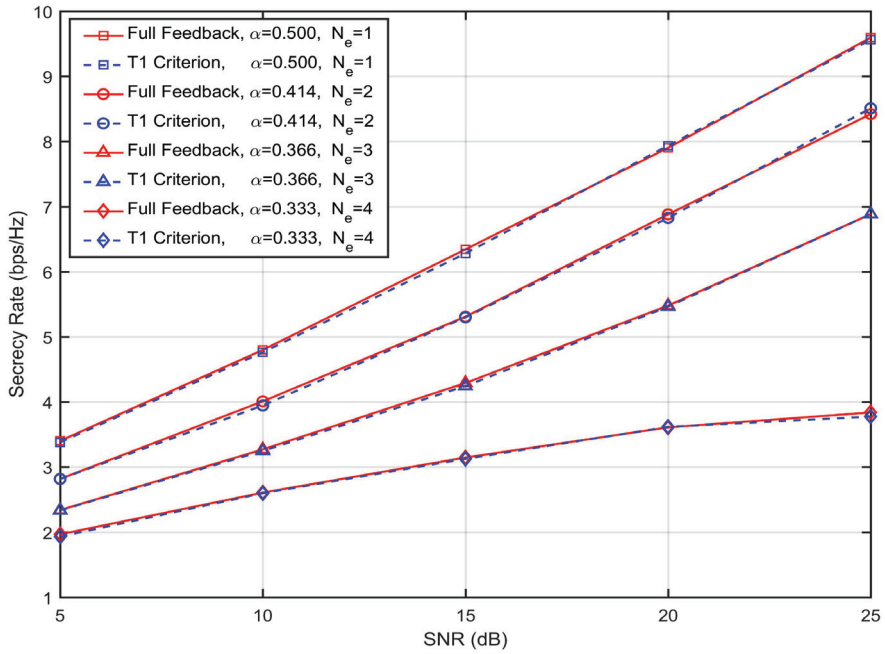

Figure 3.8. Secrecy rate versus SNR for N_e in the case of CSI of Eve is unknown and CSI of Bob is perfectly available at Alice for $K = 50$.

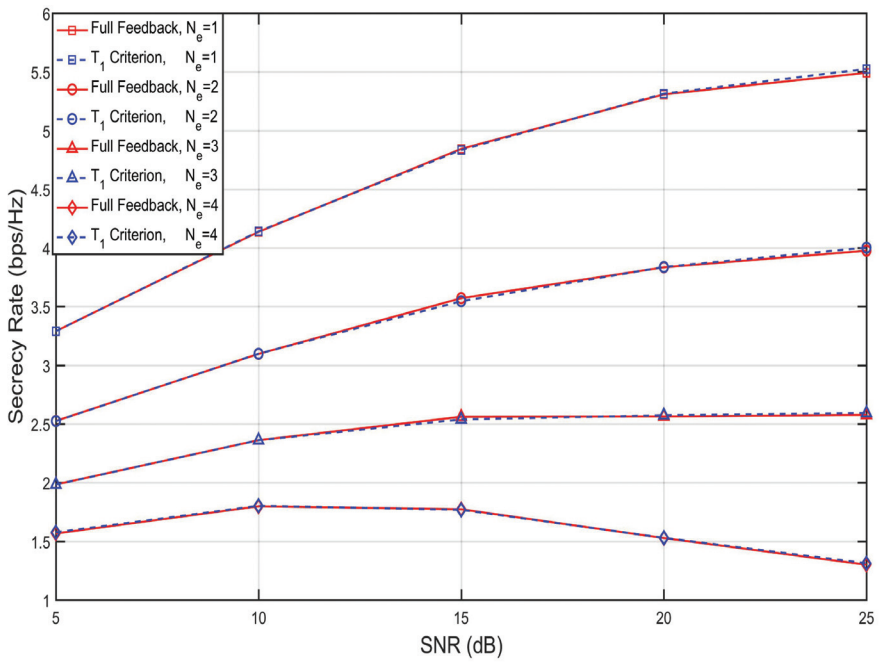

Figure 3.9. Secrecy rate versus SNR for N_e in the case of CSI of Eve is unknown and quantized version of the legitimate user's CSI ($B = 12$) is available at Alice for $K = 50$. The power allocation parameter $\alpha = 0.8$.

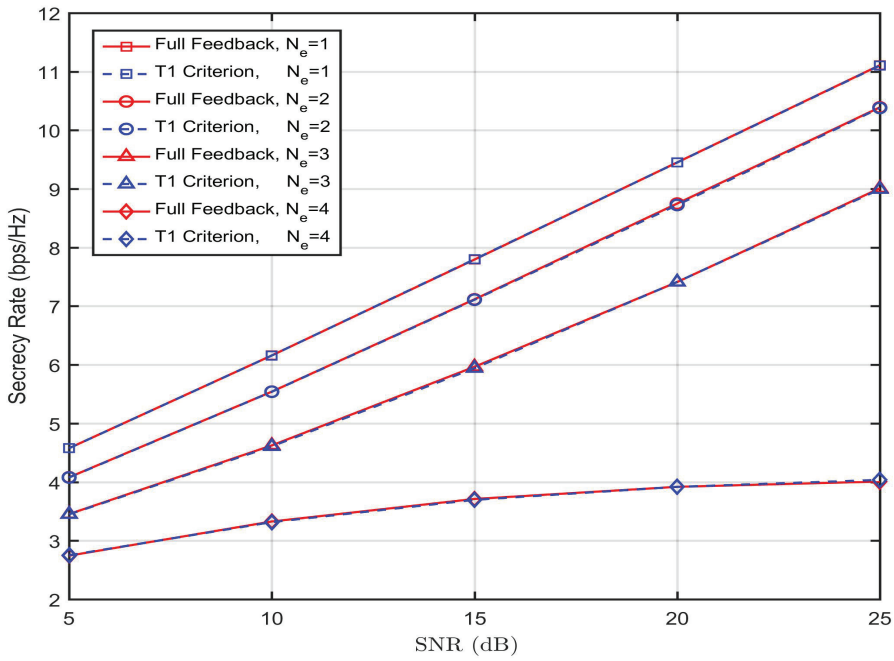

Figure 3.10. Secrecy rate versus SNR for N_e in the case of CSI of Eve is known and CSI of Bob is perfectly available at Alice for $K = 50$.

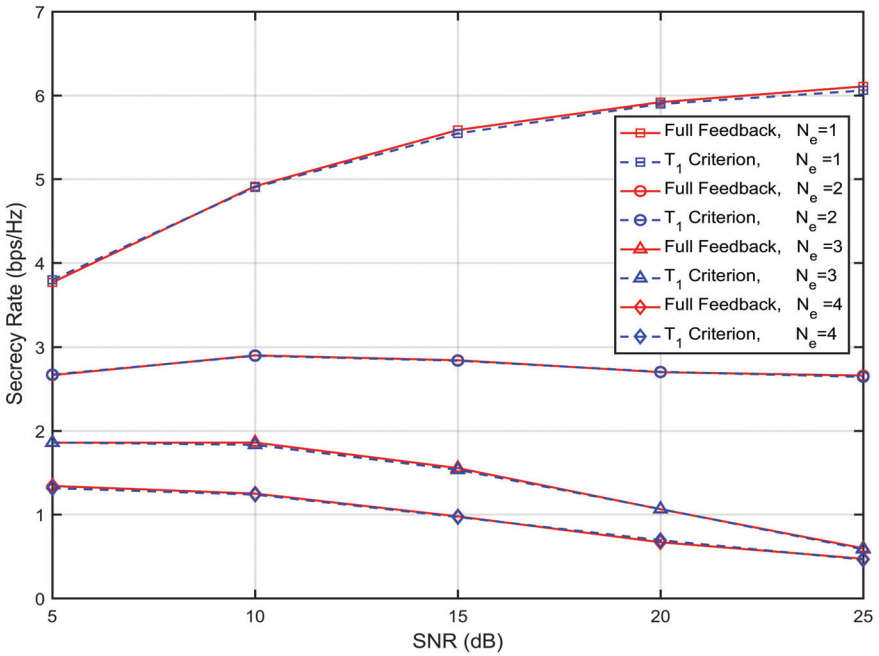

Figure 3.11. Secrecy rate versus SNR for N_e in the case of quantized version of the legitimate user's CSI and eavesdropper's CSI are available at Alice for $K = 50$. The number of quantization bits, $B = 12$ for both eavesdropper and legitimate user.

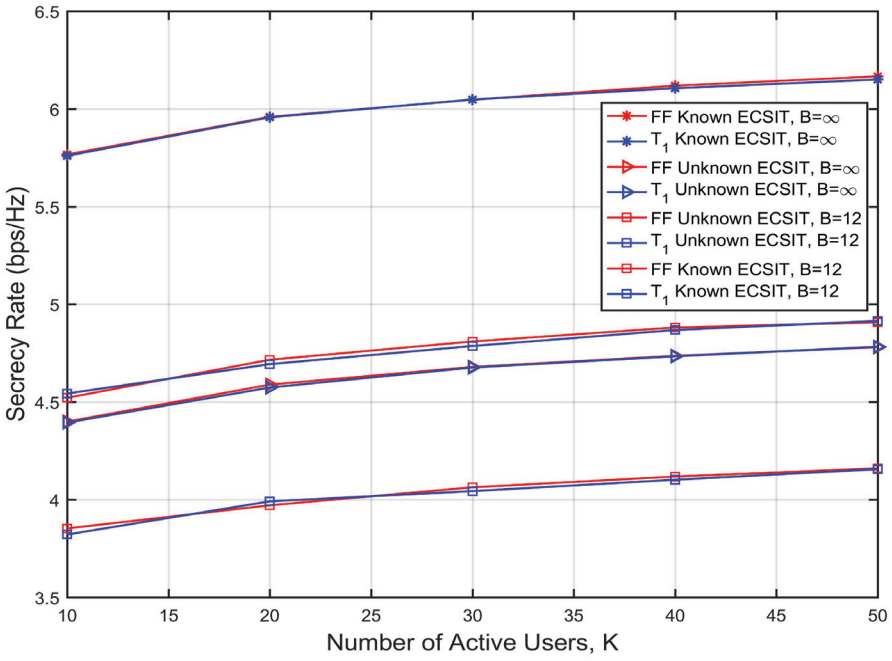

Figure 3.12. Secrecy rate versus K for different type of CSI of Eve and Bob at Alice and CSI of Bob for SNR = 10dB, $N_e = 1$.

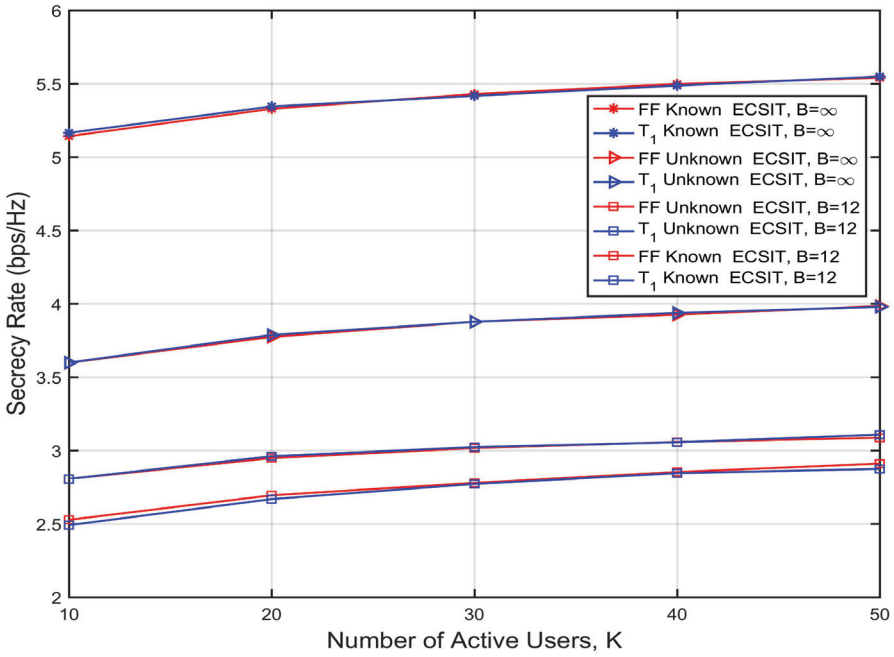

Figure 3.13. Secrecy rate versus K for different type of CSI of Eve and Bob at Alice and CSI of Bob for SNR = 10dB, $N_e = 2$.

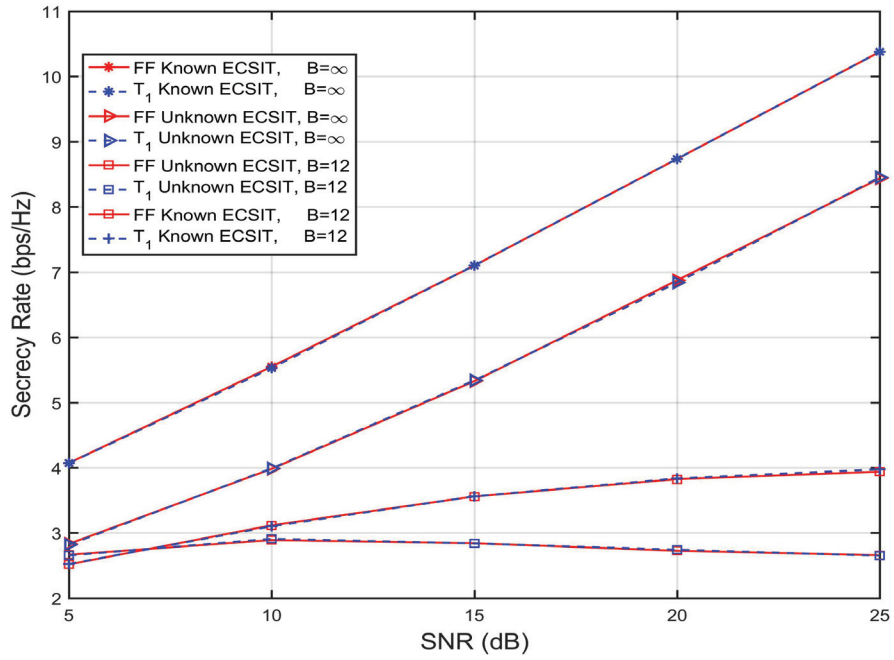

Figure 3.14. Secrecy rate versus SNR for different type of CSI of Eve and Bob at Alice and CSI of Bob for $N_e = 2$, K=50.

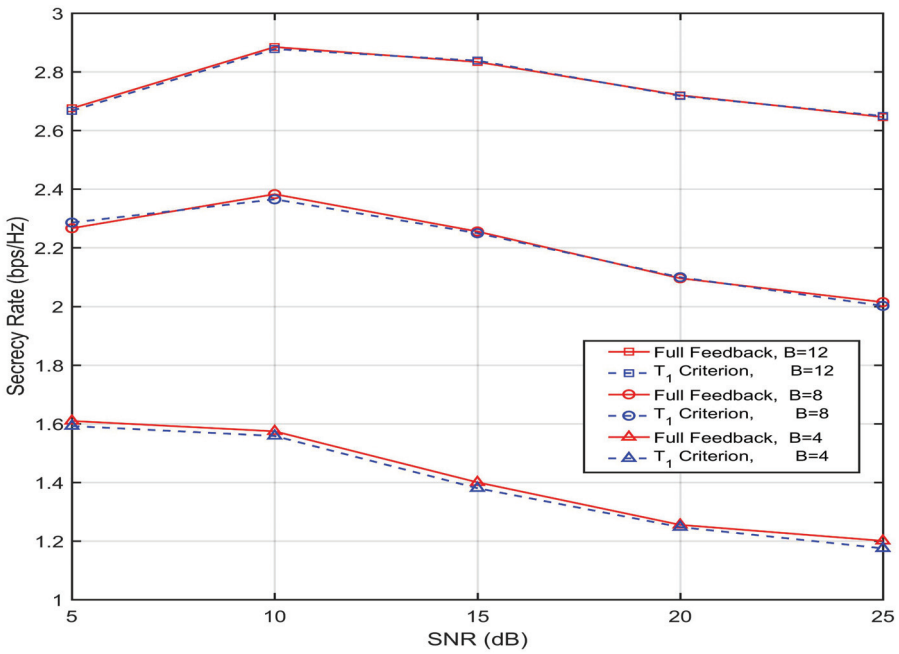

Figure 3.15. Secrecy rate versus SNR for different number of quantization bits in the case of CSI of Eve is known at Alice for N_e = 2, K = 50.

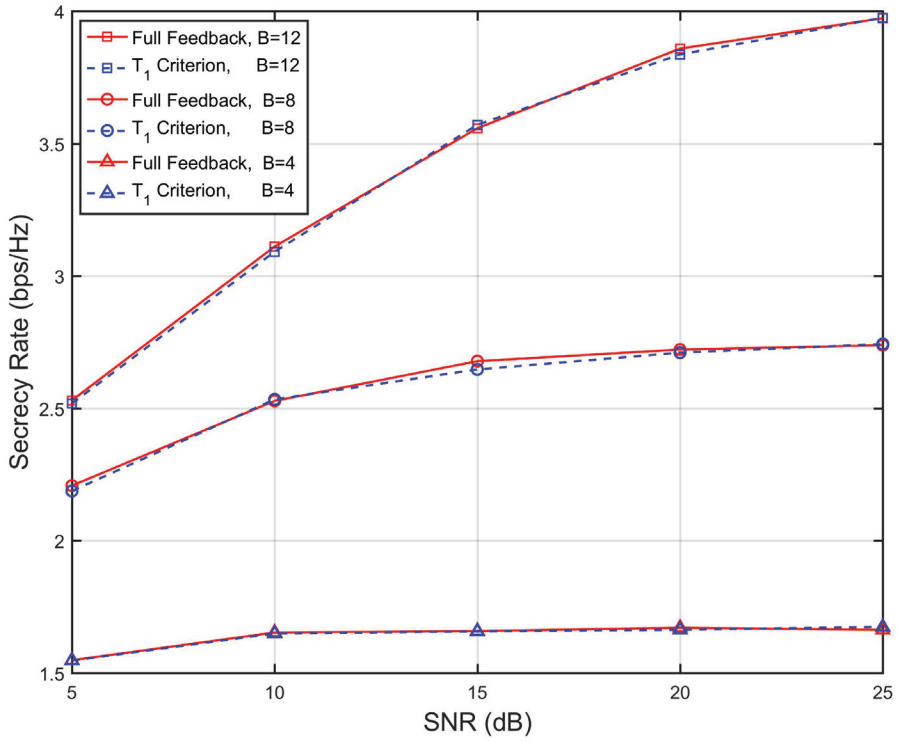

Figure 3.16. Secrecy rate versus SNR for different number of quantization bits in the case of CSI of Eve is unknown at Alice for N_e = 2, α = 0.8, K=50.

3.2. System Model for Temporally Correlated Channels

In this section, we consider a system model that consists of a transmitter with N_t antenna, one legitimate receiver with single antenna, and one eavesdropper with N_e antenna. It is assumed that transmitter can not acquire eavesdropper channel state information. Information bearing messages that are sent to the legitimate user are masked with the artificial noise signal. The purpose of employing artificial beamforming is preventing eavesdropper to decode confidential messages since positive secrecy rate is desired.

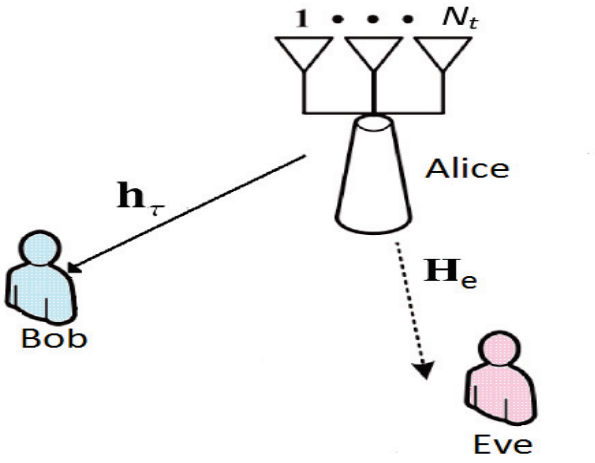

Figure 3.17. A system model that consists a multi-antenna transmitter, an legitimate receiver with single antenna and an eavesdropper with multiple-antenna

Thus, the transmitted message signal at τ time instant can be written as,

$$\mathbf{x}_\tau = \mathbf{w}_\tau s + \mathbf{Q}_\tau \mathbf{a}, \tag{3.24}$$

The beamformer that is designed via differential codebook at time instant τ is $\mathbf{w}_\tau \in C^{N_t \times 1}$. The matrix $\mathbf{Q}_\tau \in C^{(N_t-1)\times N_t}$ is the AN beamformer, and it is generated in the null space of message beamforming vector $\mathbf{w}_\tau$. The AN signal injected in null space of legitimate user to guarantee that the receiver is not affected.

The received signals at the user and eavesdropper are

$$y_\tau = \mathbf{h}_\tau^H \mathbf{w}_\tau s + \mathbf{h}_\tau^H \mathbf{Q}_\tau \mathbf{a} + n_\tau, \tag{3.25}$$

$$\mathbf{y}_{e,\tau} = \mathbf{H}_e \mathbf{w}_\tau s + \mathbf{H}_e \mathbf{Q}_\tau \mathbf{a} + \mathbf{n}_{e,\tau}. \tag{3.26}$$

The channel vector of the legitimate user is denoted as $\mathbf{h}_\tau \in C^{N_t \times 1}$. The eavesdropper's channel $\mathbf{H}_e$ is modeled with $\mathcal{CN}(0, \mathbf{I}_{N_t})$ distribution. In this section, the differential codebook is used to quantize the channel state information of the legitimate user with fading channel model. The channel is temporally correlated i.e, the channel is related to the previous time instant. The additive white Gaussian noise (AWGN) terms at the user and the eavesdropper are $\mathcal{CN}(0, \sigma^2)$ and $\mathcal{CN}(0, \sigma_e^2 \mathbf{I}_{N_e})$ respectively.

The differential codebook is a limited feedback method that aims to improve system performance using the temporal correlation of fading channels. In this method, it is assumed that the beamforming vector of the transmitter knows the previous state of a time unit and the channel is related to the time. A new beamforming vector is generated using the directional changes of the previous channel direction information and the normalized channel vector. These directional changes occurring at successive time intervals correspond to the geodesics of the Grassmannian manifold. The SNR values obtained at the legitimate user and the eavesdropper according to the beamforming vectors obtained by the codebook using the differential codebook at time τ are given respectively,

$$\gamma_\tau = \frac{\alpha |\mathbf{h}_\tau^H \mathbf{w}_\tau|^2}{\frac{1-\alpha}{N_t - 1} |\mathbf{h}_\tau^H \mathbf{Q}_\tau|^2 + \frac{1}{\rho}}, \tag{3.27}$$

$$\gamma_{e,\tau} = \alpha (\mathbf{H}_e \mathbf{w}_\tau)^H \left(\frac{1-\alpha}{N_t - 1} (\mathbf{H}_e \mathbf{Q}_\tau)(\mathbf{H}_e \mathbf{Q}_\tau)^H \right)^{-1} (\mathbf{H}_e \mathbf{w}_\tau). \tag{3.28}$$

It is assumed that no information is known regarding the channel of the eavesdropper. The secrecy capacity is defined as the maximum amount of information that can be transmitted securely to the legitimate receiver. This value is expressed as the difference of the channel capacities of the receiver and the eavesdropper (Wyner, 1994). Then, the achievable secrecy capacity is

$$C_\tau = \max\{(\mathbb{E}\{\log_2(1 + \gamma_\tau)\} - \mathbb{E}\{\log_2(1 + \gamma_{e,\tau})\}), 0\}^+. \tag{3.29}$$

3.2.1. Performance Evaluations

The performance of the differential codebook under secrecy considerations is presented. For the case of the number of antennas in the transmitter is $N_t = 4$, while the number of antennas at the user and eavesdropper are $N_r = 1$ and $N_e = 2$, respectively. The Rayleigh fading channel is designed based on the Jakes model. The channel correlation parameter is calculated by $z = J_0(2\pi f_D T)$. The J_0 corresponds to the zero-degree Bessel function from the first type. The maximum Doppler frequency is given as $f_D = \frac{v f_c}{c}$, $f_c = 2.4$ GHz, and $T = 5$

ms. Velocities of users are selected as $v = 0.45$ km/h, $v = 2.25$ km/h, and $v = 4.5$ km/h. These values correspond to the Doppler frequencies, $f_D = 1, 5, 10$ Hz, and the corresponding correlation values are $z = 0.9998, 0.9938, 0.9755$, respectively.

The full CSI expression used for comparison in the simulations is that the CSI at the transmitter can be obtained perfectly ($B = \infty$). In practice, however, this is not possible as the feedback channels are limited. This requires the use of codebook based methods. The initial full CSI case is that the CDI at the time zero is perfectly known to the receiver and then it is not updated in time.

In Figure 3.18, the change of channel amplitude in time is depicted for $f_D = 5$. In Figures from Figure 3.19 to Figure 3.22, secrecy capacity results for SNR, $\gamma = 10$ dB at different velocities are shown. It is observed that the differential codebook yields much better results than RVQ. Figure 3.19 and Figure 3.20 show the fact that differential codebook vectors can follow the actual channel direction successfully at low velocities ($v = 0.45$km/h). For different size of polar cap δ_τ values, the capability and speed of tracking channel direction is also varies. As observed from Figure 3.21, Figure 3.22, it is not enough to only have initially perfect CSI in higher velocities. In these cases, secure communications can not be guaranteed by using initial perfect CSI only. Besides, if the size of polar cap δ_τ is chosen small, it can not track the CDI correctly. The size of δ_τ must be selected optimally to give highest achievable secrecy rate.

In Figures, from Figure 3.23 to Figure 3.26, the secrecy capacity results for SNR, $\gamma = 20$ dB at different velocities are presented. In these results, the performance of initial perfect CSI at $\gamma = 20$ dB is worse than $\gamma = 10$ dB case. The performance of differential codebook is almost same in the case of $\gamma = 10$ dB, and secrecy rate is increased with $\gamma = 20$ dB.

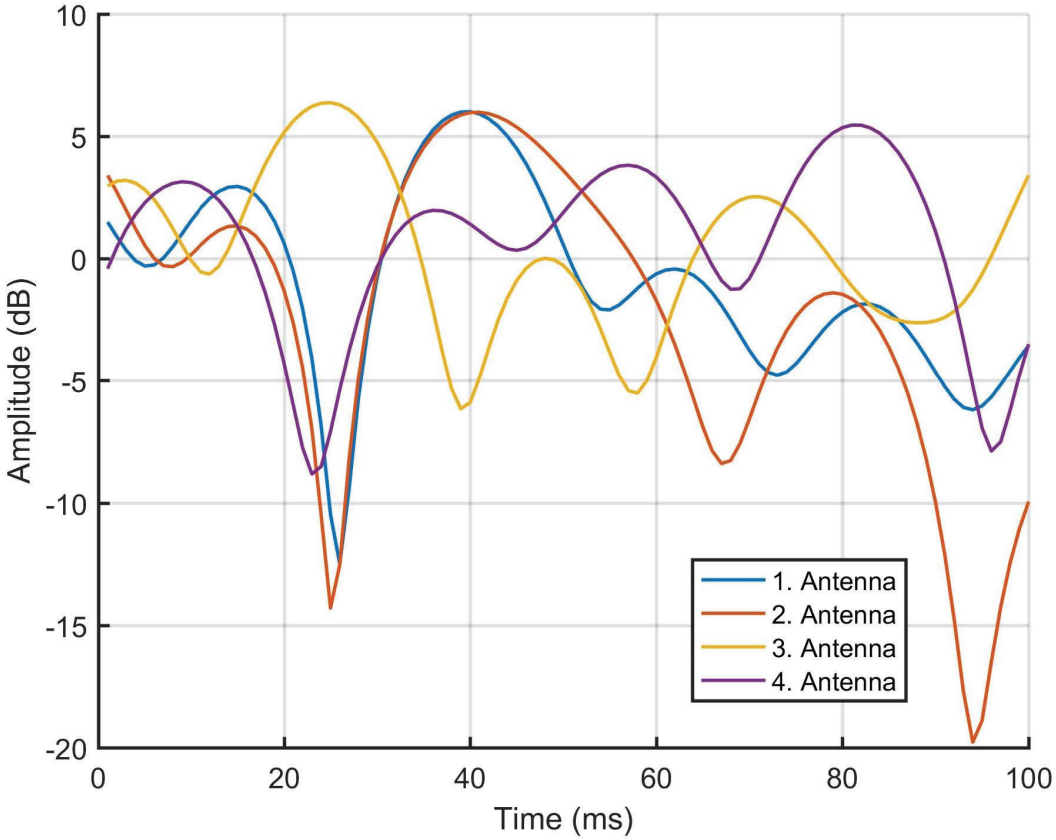

Figure 3.18. Channel Amplitudes versus Time for f_D = 5 Hz

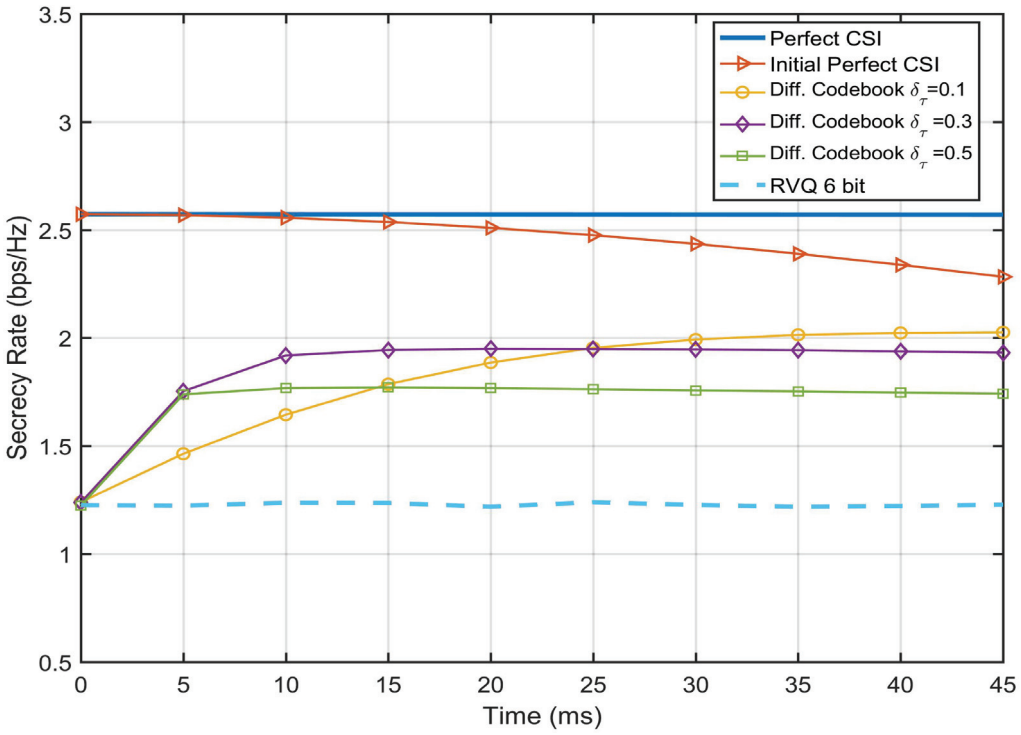

Figure 3.19. Secrecy rate versus time for $\gamma = 10$dB, $f_D = 1$ Hz.

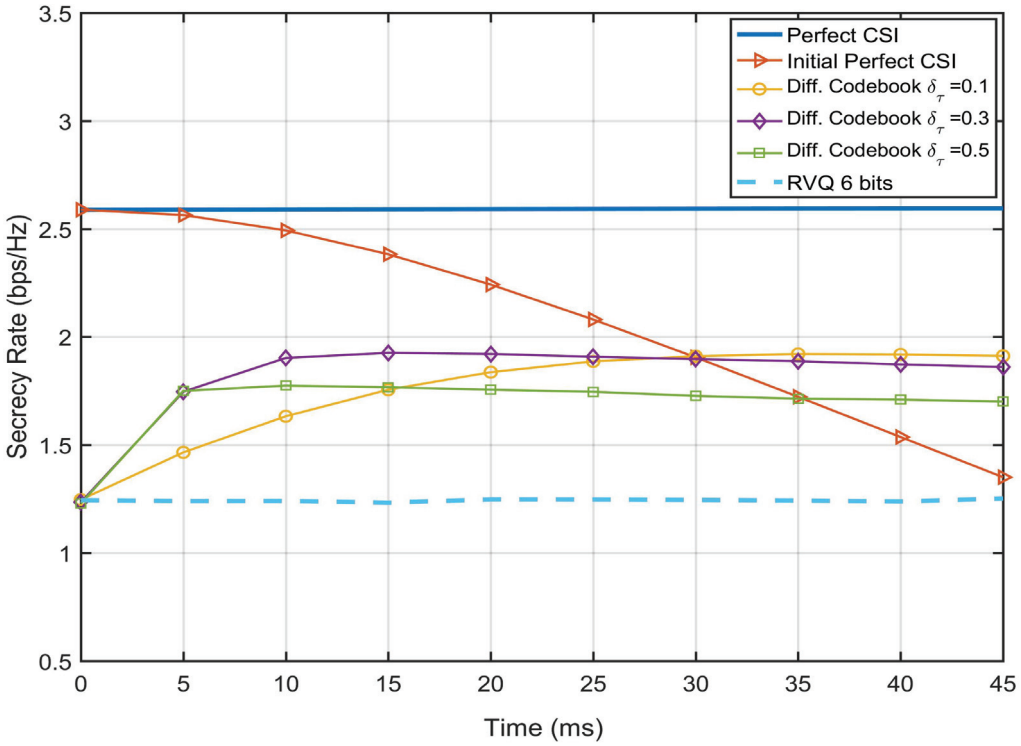

Figure 3.20. Secrecy rate versus time for $\gamma = 10$dB, $f_D = 2.5$ Hz.

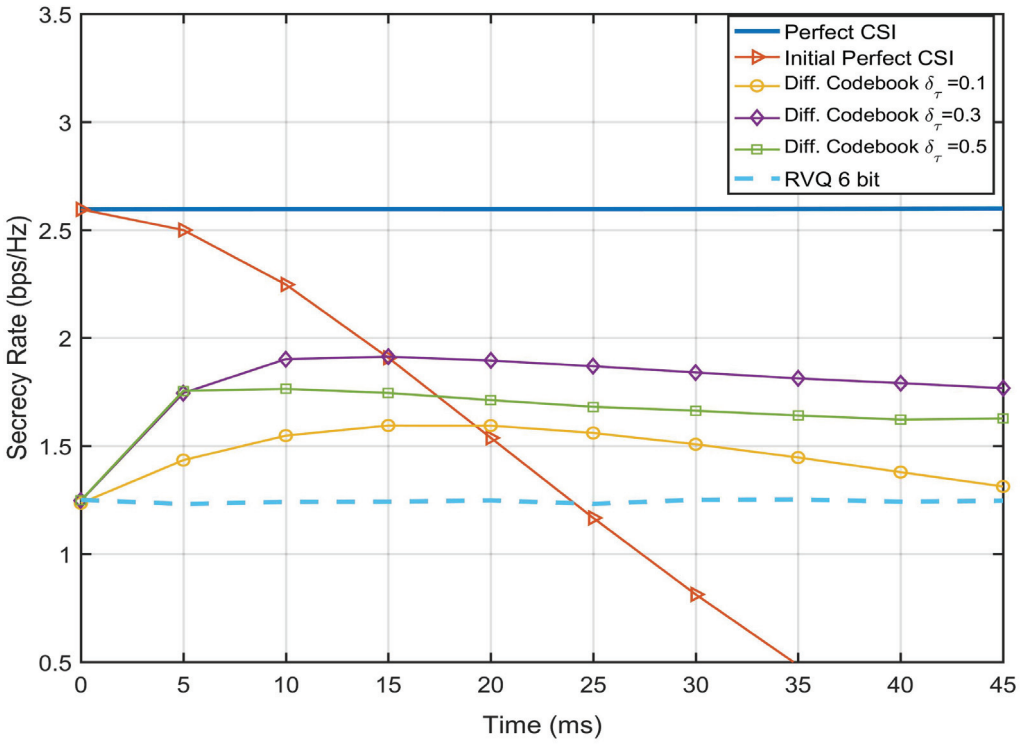

Figure 3.21. Secrecy rate versus time for $\gamma = 10$dB, $f_D = 5$ Hz.

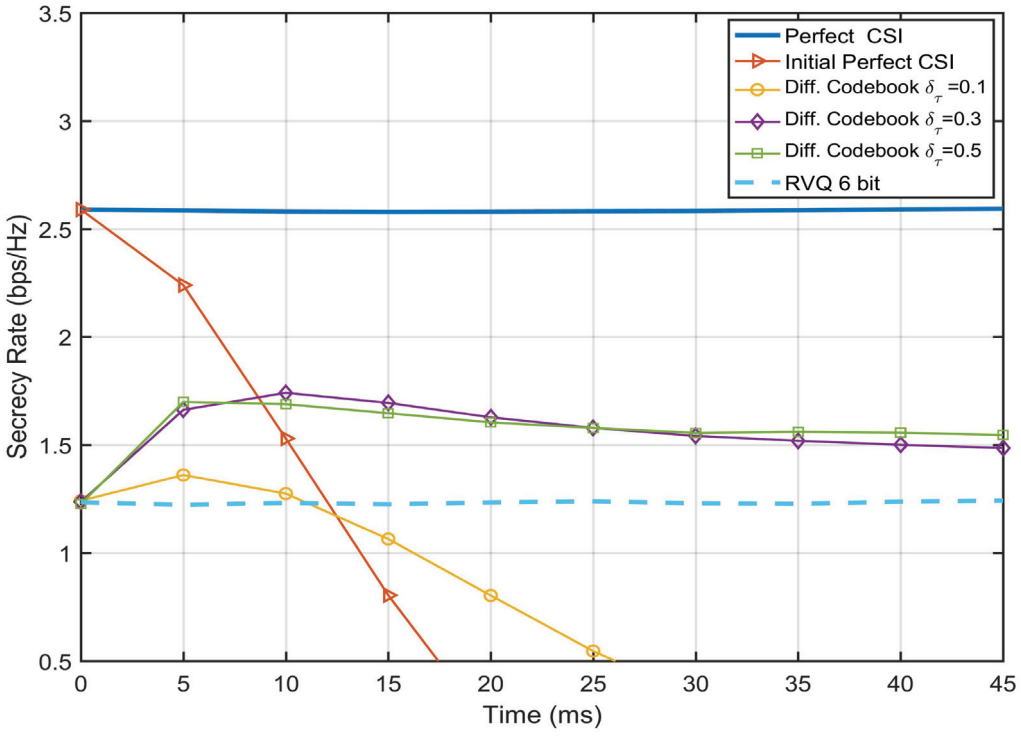

Figure 3.22. Secrecy rate versus Time for $\gamma = 10$dB, $f_D = 10$ Hz.

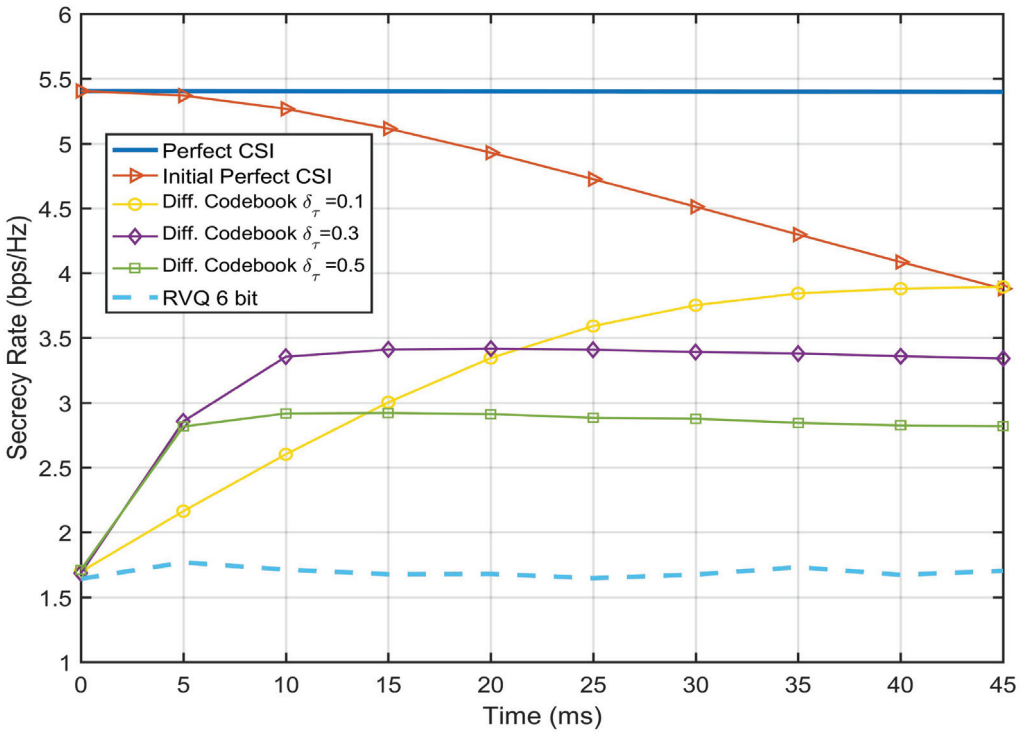

Figure 3.23. Secrecy rate versus time for $\gamma = 20$dB, $f_D = 1$ Hz.

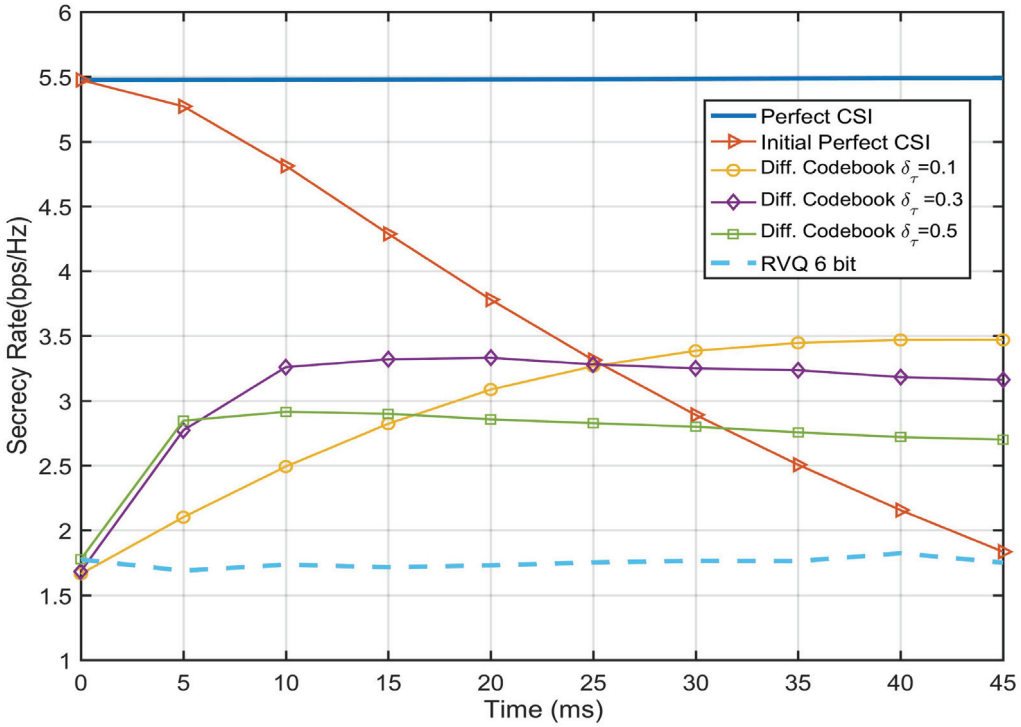

Figure 3.24. Secrecy rate versus time for $\gamma = 20$dB, $f_D = 2.5$ Hz.

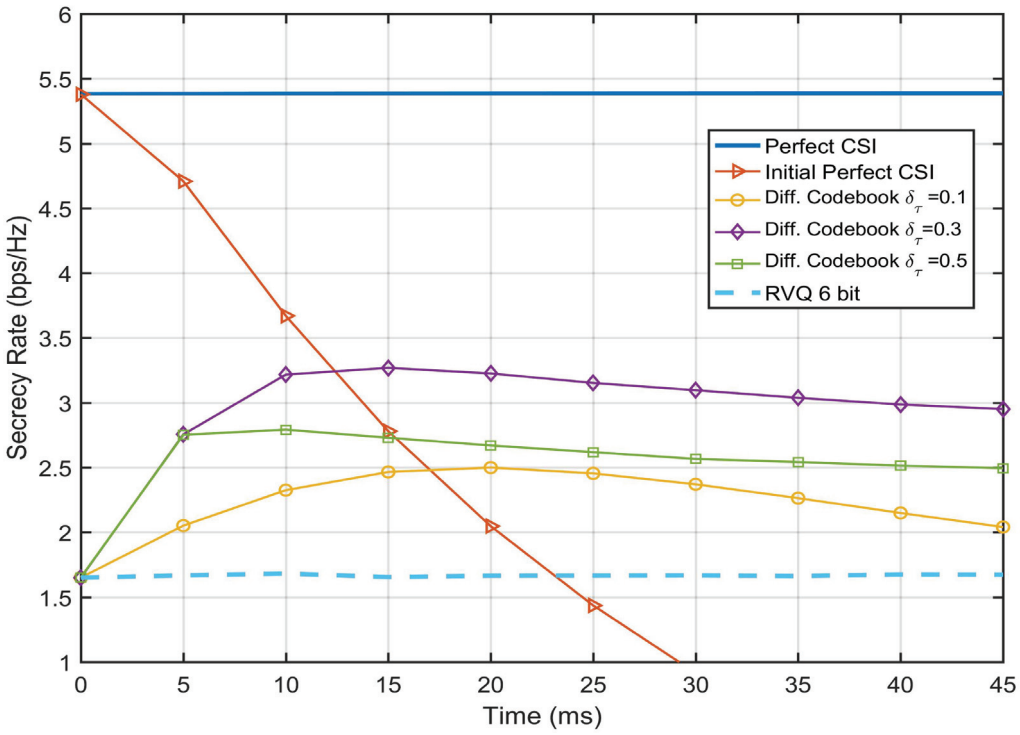

Figure 3.25. Secrecy rate versus time for $\gamma = 20$dB, $f_D = 5$Hz.

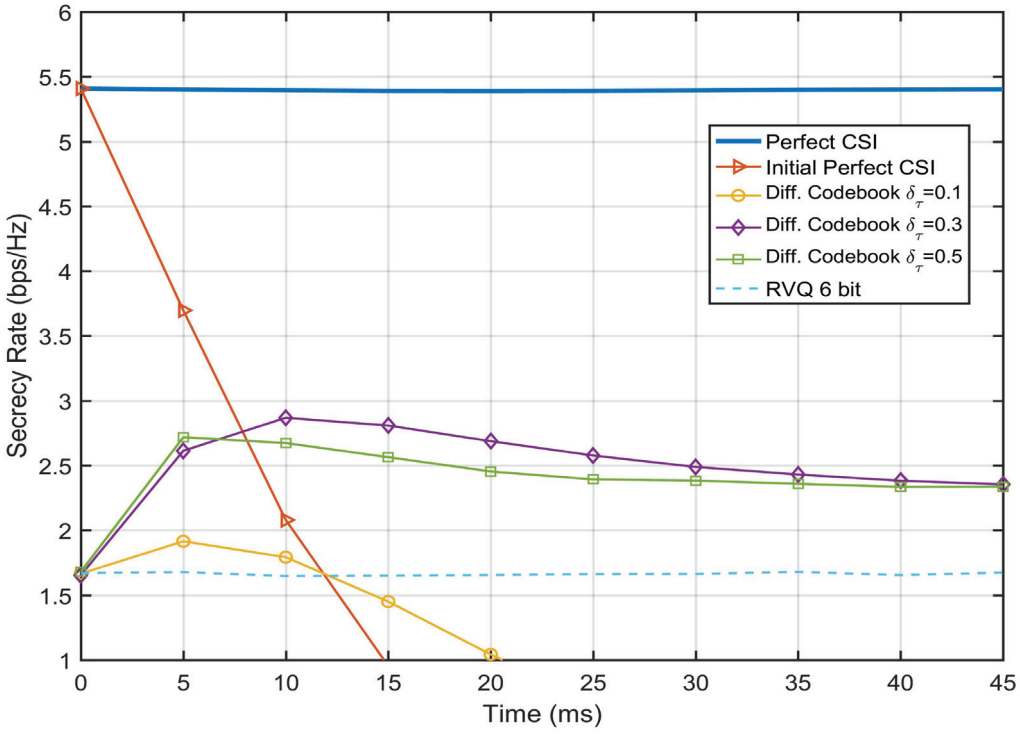

Figure 3.26. Secrecy rate versus time for $\gamma = 20$dB, $f_D = 10$ Hz.

CHAPTER 4

SECURE MULTIUSER MULTIPLE INPUT SINGLE OUTPUT SYSTEMS

In this chapter, two different secure multiuser MISO system models with passive eavesdroppers equipped with different number of antennas are studied. In both model, the problem of physical layer security is considered under limited CSI feedback link. The first system model examines Eve with single antenna. In this case, inter-user interference is used instead of artificial noise, since Eve can not eliminate it (Ozbek et al., 2016). The second system model considers the case of multiple antenna eavesdropper. The multiple antenna eavesdropper can corresponds to an alliance of N_e geographically dispersed but perfectly colluding single antenna eavesdroppers. In this case, artificial noise signal is required to jam eavesdroppers, since worst case that Eve can cancel interference from other users (Ozdogan et al., 2017b).

4.1. System model for Single Antenna Eavesdropper

We consider a multiuser MISO downlink system operating under secrecy constraints. The transmitter is equipped with N_t transmit antennas. The aim of the transmitter is to send confidential messages to intended $M \leq N_t$ legitimate users for secure communication from the set of active $K > M$ users. Also, there is an eavesdropper who aim to attain information from these scheduled M users. The eavesdropper is passive and its CSI is not available at the transmitter. Besides, we assume that the transmitter only has partial CSI of legitimate users. All these K legitimate users and the eavesdropper have only one receive antenna.

The transmitted signal $\mathbf{x}$ at Alice is expressed as,

$$\mathbf{x} = \hat{\mathbf{W}}\mathbf{s}, \tag{4.1}$$

where $\mathbf{s} = [s_1, s_2, \ldots, s_M]$ is an information symbol vector with $\mathbb{E}\{||\mathbf{s}||^2\} \leq P$ and $\hat{\mathbf{W}} = [\hat{\mathbf{w}}_1, \hat{\mathbf{w}}_2 \ldots, \hat{\mathbf{w}}_m, \ldots, \hat{\mathbf{w}}_M]$ is the precoding matrix generated by employing ZFBF as $\hat{\mathbf{W}} = \hat{\mathbf{H}}(\mathbb{M})^H(\hat{\mathbf{H}}(\mathbb{M})\hat{\mathbf{H}}(\mathbb{M})^H)^{-1}$. The channel matrix, $\hat{\mathbf{H}}(\mathbb{M}) \in C^{M \times N_t}$, includes channel vectors of scheduled legitimate users as $\hat{\mathbf{H}}(\mathbb{M}) = [\hat{\mathbf{h}}_1, \hat{\mathbf{h}}_2 \ldots, \hat{\mathbf{h}}_m, \ldots, \hat{\mathbf{h}}_M]^T$ with $\hat{\mathbf{h}}_m$ is the quantized ver-

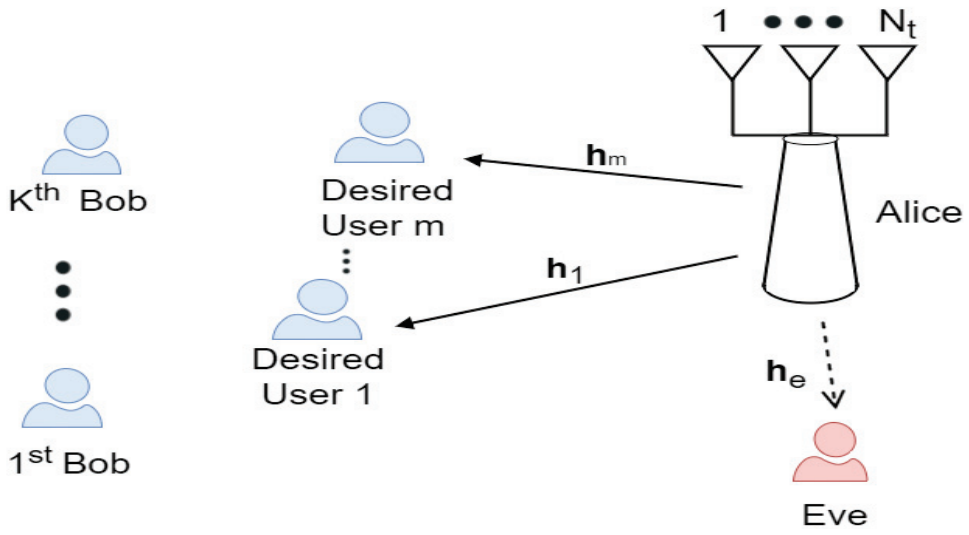

Figure 4.1. A system model that consists a multi-antenna transmitter, K legitimate receivers with single antenna and an eavesdropper with single antenna

sion of channel vector of m^{th} legitimate user. This channel vector, $\mathbf{h}_m \in C^{N_t \times 1}$, is modelled by $C\mathcal{N}(0, \mathbf{I})$. The columns of $\hat{\mathbf{W}}$ is normalized as $\|\hat{\mathbf{w}}_m\| = 1$. Thus, we send confidential messages to M scheduled legitimate users simultaneously while mitigating inter-user interference by ZFBF.

In order to address the lack of perfect CSI for Bobs at the transmitter, it is possible to quantize CDI, $\mathbf{g}_k$, and CQI, $\|\mathbf{h}_k\|$ as described in Section 2.3. In this thesis, we assume that CQI is perfectly known at the transmitter. Therefore, each legitimate user quantizes its CDI to an unit norm vector selected from a predetermined codebook.The M best legitimate users based on their channel norm are scheduled at Alice.

Then, the received signal at the m^{th} Bob is written as,

$$\hat{y}_m = \|\mathbf{h}_m\|(\bar{\mathbf{h}}_m^H \hat{\mathbf{w}}_m)s_m + \sum_{j=1, j\neq m}^{M} \|\mathbf{h}_m\|(\bar{\mathbf{h}}_m^H \hat{\mathbf{w}}_j)s_j + n_m, \tag{4.2}$$

where n_m is additive white Gaussian noise (AWGN) with zero mean and variance of σ^2. The received signal belonging to the m^{th} Bob at Eve is expressed by

$$\hat{y}_{e_m} = \mathbf{h}_e^H \hat{\mathbf{w}}_m s_m + \sum_{j=1, j\neq m}^{M} \mathbf{h}_e^H \hat{\mathbf{w}}_j s_j + n_e. \tag{4.3}$$

where n_e is AWGN with zero mean and variance of σ_e^2. The signal-to-interference-noise ratio (SINR) at m^{th} Bob is written as,

$$\hat{\gamma}_m = \frac{\frac{P}{M}||\mathbf{h}_m||^2|\bar{\mathbf{h}}_m^H\hat{\mathbf{w}}_m|^2}{\sum_{j=1,j\neq m}^{M}\frac{P}{M}||\mathbf{h}_m||^2|\bar{\mathbf{h}}_m^H\hat{\mathbf{w}}_j|^2+\sigma^2}, \tag{4.4}$$

The SINR at Eve belonging to the m^{th} Bob is given by,

$$\hat{\gamma}_{e_m} = \frac{\frac{P}{M}\,|\mathbf{h}_e^H\hat{\mathbf{w}}_m|^2}{\sum_{j=1,j\neq m}^{M}\frac{P}{M}\left|\mathbf{h}_e^H\hat{\mathbf{w}}_j\right|^2}. \tag{4.5}$$

Then, the secrecy sum capacity under quantized CDI is determined in the following:

$$R = \left(\sum_{m=1}^{M}\mathbb{E}\left\{\log_2\left(1+\hat{\gamma}_m\right)\right\} - \mathbb{E}\left\{\log_2\left(1+\hat{\gamma}_{e_m}\right)\right\}\right)^+. \tag{4.6}$$

Since $\hat{\mathbf{W}}$ is not perfectly orthogonal to the channel of legitimate users, inter-user interference negatively affects the reception of Bobs. In the meantime, inter-user interference disturbs the reception of the Eve. In order to reduce the quantization error of legitimate users, semi-orthogonal selection criterion with specific codebook at receiver side is applied in this thesis. Due to the fact that inter-user interference can not be completely eliminated, the reception of Eve is still degraded in the proposed solution.

4.2. The semi-orthogonal selection with rotated codebook

In order to maximize the secrecy sum capacity of the downlink MISO system while achieving multiuser diversity, it is necessary to select the best combinations of M legitimate users. Therefore, the legitimate users having poor channel condition (have low norm and/or causes high inter-user interference) should not take part in the scheduling algorithm, nor feedback their CSI.

Inter-user interference is a pivotal factor in classical multiuser communications. It may have a positive impact for secure multiuser systems since it causes interference to eavesdropper transmission. Therefore, the selection criterion at the Bobs' side is very critical to improve secrecy sum capacity. Only selected users are fed back their CSI to Alice by using a specific codebook that is called as rotated codebook. Along with that, we schedule best M

legitimate users according to their norms to achieve higher secrecy sum capacity.

The semi-orthogonal criterion selects the legitimate users whose CDI are semi-orthogonal. Each Bob generates the same N_t random orthonormal vectors as $\phi_i \in C^{N_t \times 1}$, $i = 1, \ldots, N_t$. Then, they measure the orthogonality between their channels and ϕ_i using the chordal distance:

$$d^2(\mathbf{g}_k, \phi_i) = 1 - |\mathbf{g}_k^H \phi_i|^2 \tag{4.7}$$

Let $\mathcal{O}^{N_t}$ be the unit sphere lying in $\mathbb{C}^{N_t}$ and centered at the origin. Using the chordal distance metric, for any $0 < \epsilon < 1$, we can define a spherical cap on $\mathcal{O}^{N_t}$ with center $\mathbf{o}$ and square radius ϵ as the open set :

$$\mathcal{B}_\epsilon(\mathbf{o}) = \left\{ \mathbf{g}_k \in \mathcal{O}^{N_t} : d^2(\mathbf{g}_k, \mathbf{o}) \leq \epsilon \right\} \tag{4.8}$$

Then, we apply the criterion $\mathcal{T}_3$ as described in the following (Ozbek and Le Ruyet, 2014):

$$\mathcal{T}_3 = \left\{ k \in K : \mathbf{g}_k \in \bigcup_{i=1}^{N_t} \mathcal{B}_\epsilon(\phi_i) \text{ and } \|\mathbf{g}_k\|^2 \geq \gamma_{th} \right\} \tag{4.9}$$

where ϵ is the threshold on semi-orthogonality criterion and γ_{th} is the threshold on norm. Thus, the legitimate users which satisfy semi-orthogonality condition but having low norm should not take part in scheduling for reason that channel quality of selected Bobs directly affects the secrecy sum capacity.

Consequently, $\bar{K}$ Bobs on average are allowed to fed back their CSI to Alice whose schedules M legitimate users with the highest norm to establish secure transmission. The threshold values are determined to have $\bar{K}$ legitimate users in average in limited feedback link by,

$$\bar{K} = KN_t \sum_{b=0}^{N_t-1} \frac{\exp(-\gamma_{th})(\gamma_{th})^b}{b!} \epsilon^{N_t-1} \tag{4.10}$$

In order to reduce the quantization error of the legitimate users selected by the criterion $\mathcal{T}_3$, we use a specific codebook based on the quantization of the localized region (Ozbek and Le Ruyet, 2014) instead of the normalized independent and identically distributed (i.i.d) channel in isotropically distributed in $\mathcal{O}^{N_t}$.

As in the i.i.d. case, we use a practical vector quantization scheme to design the local packings. For the $\mathcal{T}_3$ criterion, the codebook is designed according to the orthogonal vectors ϕ_i. From the local packing associated to the spherical cap $\mathcal{B}_\epsilon(\mathbf{o})$, it is possible to compute $\mathcal{B}_\epsilon(\phi_i)$ using the rotation matrix:

$$\phi_i = \mathbf{U}_r \mathbf{o} \tag{4.11}$$

where $\mathbf{U}_r$ is the unitary rotation matrix.

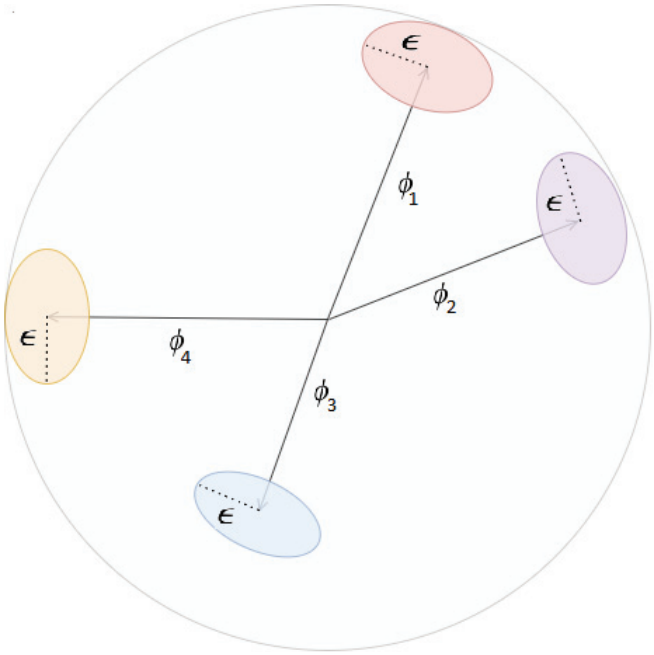

Figure 4.2. A geometric interpretation of rotated codebook

The Figure 4.2 illustrates rotated codebook caps for $N_t = 4$ There are four randomly generated orthonormal vectors ϕ_i, where $i = 1, \ldots, 4$. The codebook only quantizes the regions that is inside the spherical cap with radius ϵ. Since, $\mathcal{T}_3$ criterion selects the users in that proximity only these users feedback their CSI.

4.3. Performance Evaluations

We illustrate the simulation results for $N_t = 2$ transmit antennas at Alice. The pair of (γ_{th}, ϵ) for $\mathcal{T}_3$ criterion is calculated to have an average number of users in the cell $\bar{K} = 4$. Then, the pairs are chosen as $[(1.65, 0.4), (2, 0.25), (2.3, 0.2), (2.55, 0.18), (2.6, 0.15)]$. Only the legitimate users that satisfy these thresholds are fed back their B bits corresponding to the codebook index of their quantized CDI to Alice. Exploiting the feedback information, Alice schedules the M legitimate users by performing ZFBF to reduce inter-user interference. In this work, the worst case scenario which means that no knowledge about CSI of Eve is available at Alice is considered.

For secure single user MISO systems with perfect CSI case, the power is shared equally between message signal and AN as an optimal manner. However, for the quantized case, as shown in Figure 4.3 at SNR=10dB and Figure 4.4 at SNR 20=dB, when the number of quantization bits are reduced, the power allocation parameter α should be increased to

maximize secrecy capacity. As a result, as the number of quantization bits reduces, most of the available power at transmitter should be used for transmitting information message rather than AN.

The secrecy sum capacity comparison for $\mathcal{T}_3$ criterion with semi orthogonal selection and full feedback case in which all users are fed back their CSI without any selection at the legitimate user side are illustrated in Figure 4.5 and Figure 4.6 depending on the number of active users and signal-to-noise ratio (SNR) with using RVQ. In Figure 4.7, the feedback load is compared for full feedback and $\mathcal{T}_3$ criterion. The overhead is reduced from 60% to 92% through $\mathcal{T}_3$ criterion based on the number of the active legitimate users in the system in the expense of reduction on secrecy sum capacity between 0.1bps/Hz and 1bps/Hz. It is observed that when the number of quantization bits are increased, the gap on secrecy sum capacity for full feedback and $\mathcal{T}_3$ criterion is also increased.

In Figure 4.8 and Figure 4.9, we compare the secrecy sum capacity for $\mathcal{T}_3$ criterion with Rotated Codebook. The performance results indicate that the secrecy sum capacity improves between 2.1bps/Hz and 0.4bps/Hz depending on the number of quantization bits for $K = 50$ by employing the special codebook. When the number of quantization bits is increased, the gain on secrecy sum capacity becomes low since the disturbance effect of inter-user interference on Eve is also reduced. Since the secrecy sum capacity is improved significantly especially at low feedback load, the semi-orthogonal criterion with a special codebook leads to a promising solution for practical applications.

In Figure 4.10, we compare the secrecy capacity for the system that performs semi-orthogonal selection having specific codebook and the system that schedules only one legitimate user with AN having the optimal power allocation based on Figure 4.4. The performance results are shown that the proposed solution for multiuser MISO system provides much better secrecy capacity performance than single user MISO system while requiring much less overhead through feedback link.

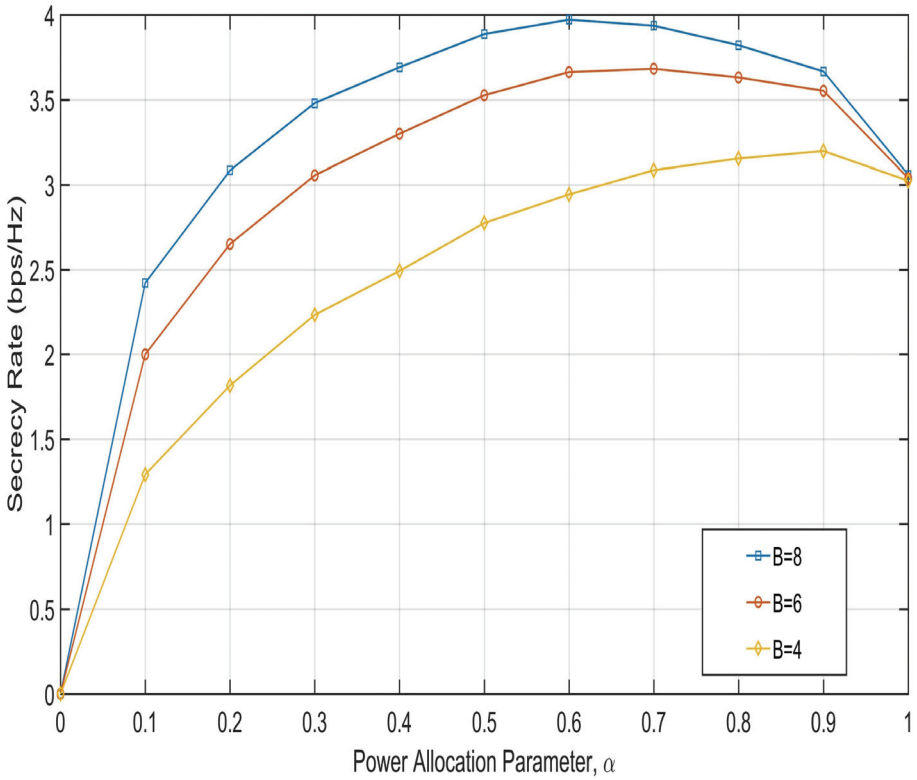

Figure 4.3. Power allocation parameter for different number of bits in single user MISO at SNR= 10dB.

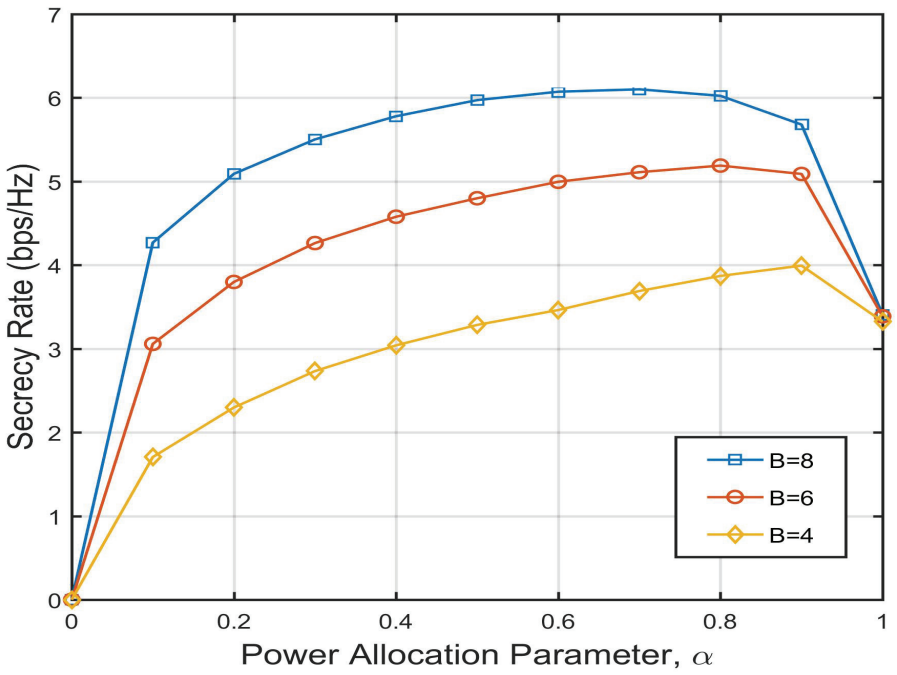

Figure 4.4. Power allocation parameter for different number of bits in single user MISO at SNR= 20dB.

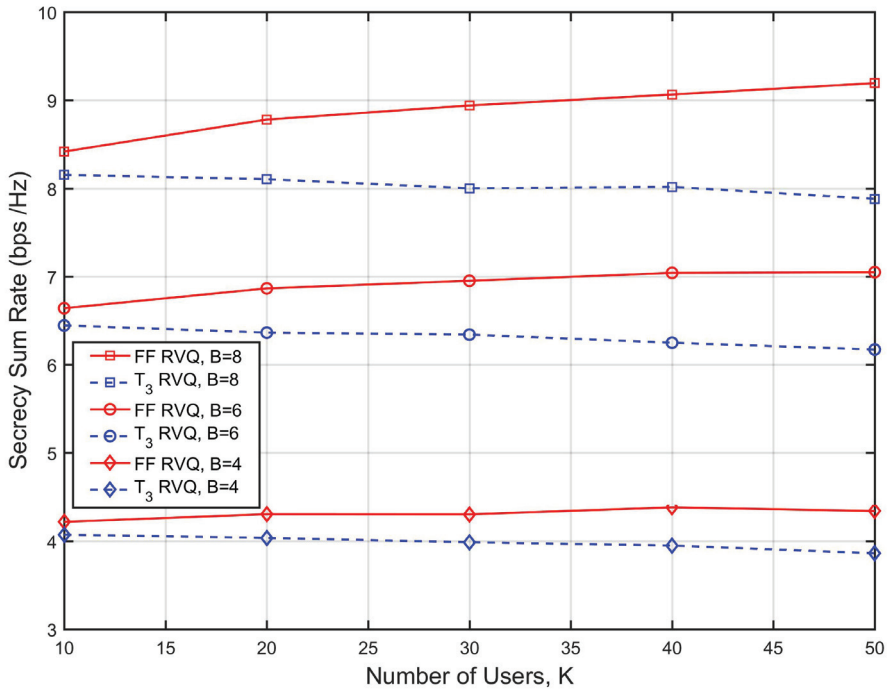

Figure 4.5. The comparison between full feedback and $\mathcal{T}_3$ criterion at SNR=20dB for the different number of active users.

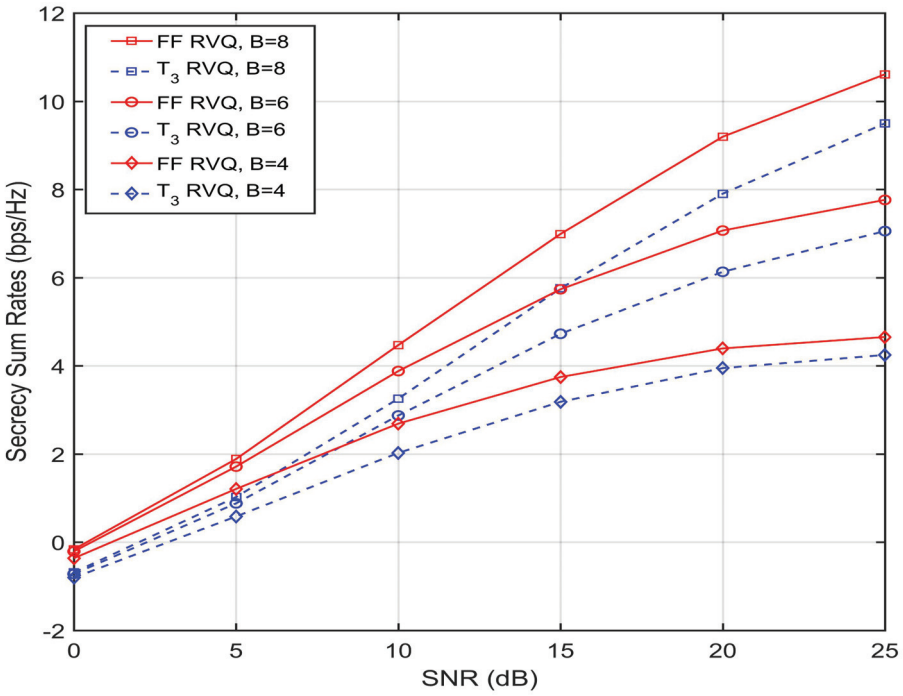

Figure 4.6. The comparison between full feedback and $\mathcal{T}_3$ criterion at $K = 50$ for different SNR values.

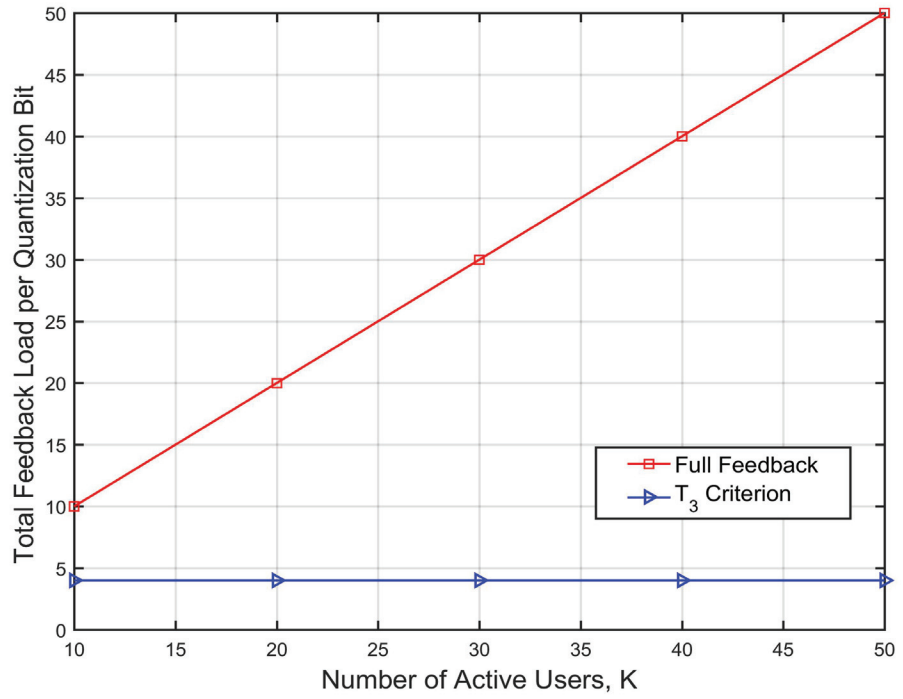

Figure 4.7. The total feedback load per the number of feedback bit for full feedback and $\mathcal{T}_3$ criterion.

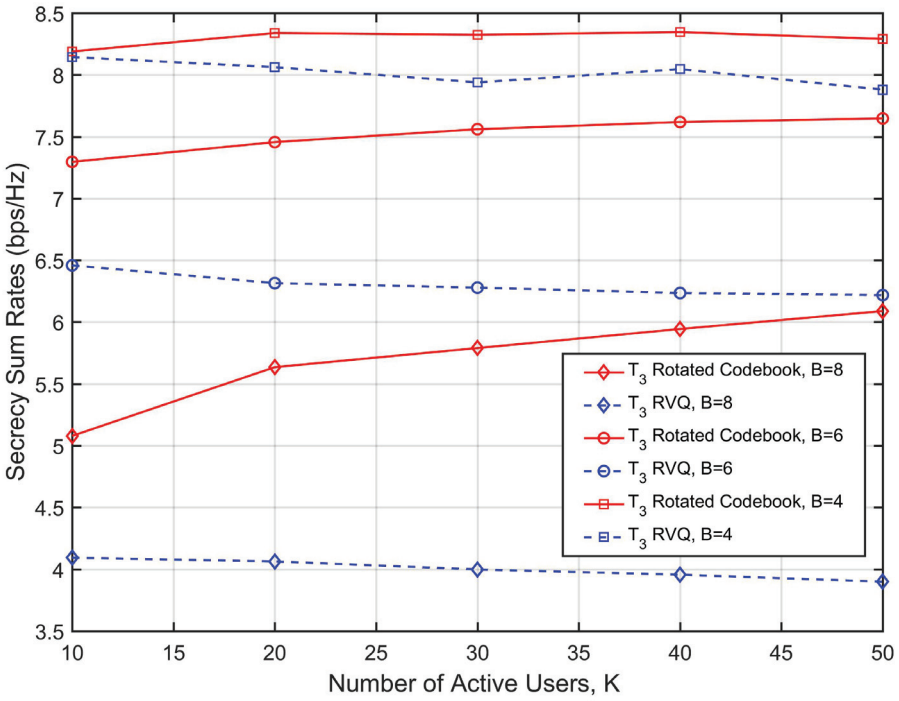

Figure 4.8. The comparison between $\mathcal{T}_3$ criterion with and without Rotated Codebook for SNR= 20dB.

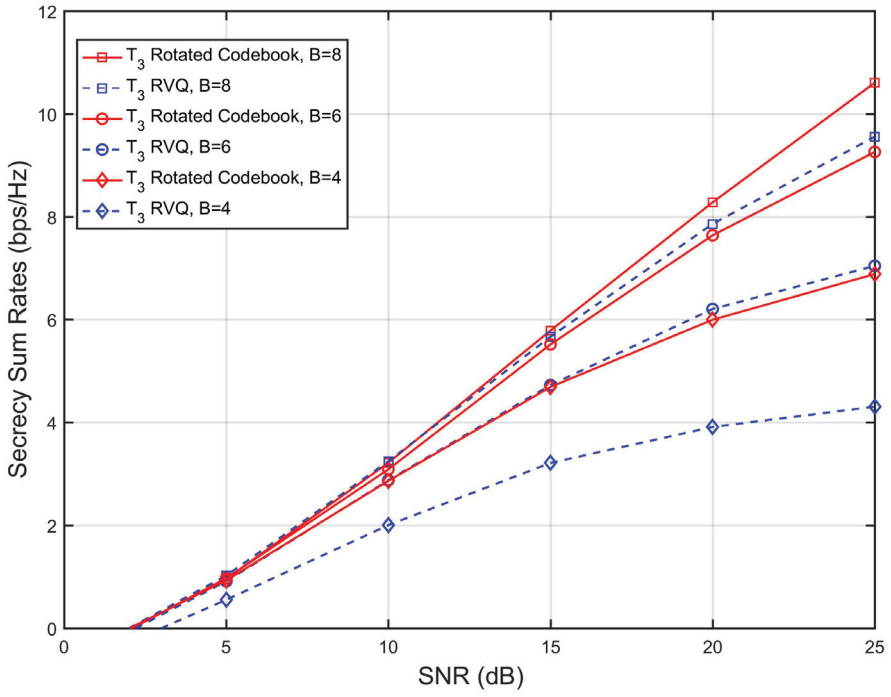

Figure 4.9. The comparison between $\mathcal{T}_3$ criterion with and without proposed codebook at $K = 50$ for different SNR values.

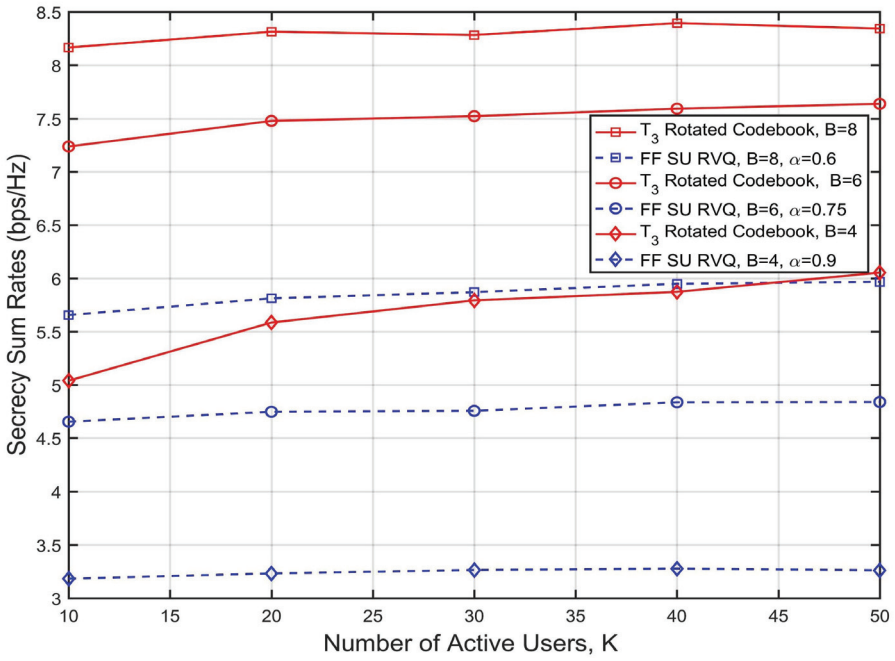

Figure 4.10. The comparison between single user MISO with full feedback (FF) case and multiuser MISO with $\mathcal{T}_3$ criterion and special codebook at SNR= 20dB.

4.4. System Model for Multiple Antenna Eavesdropper

Consider a multiuser MISOME downlink system operating under secrecy constraint. The system consists of one base station with N_t antennas, K active users each has single antenna and an eavesdropper with N_e antennas. The aim of the transmitter is to send confidential messages to intended M legitimate users which are selected for secure communication from the set of active K users ($K \geq N_t > M$). The eavesdropper overhears the secret messages illegally. We assume that legitimate users' CSI is perfectly estimated at receiver side. However, transmitter only has quantized CSI of legitimate users due to the limited feedback. Also, the transmitter has no knowledge regarding ECSIT, which is highly probable scenario in practical cases. Since, eavesdroppers are passive and they do not reveal their location.

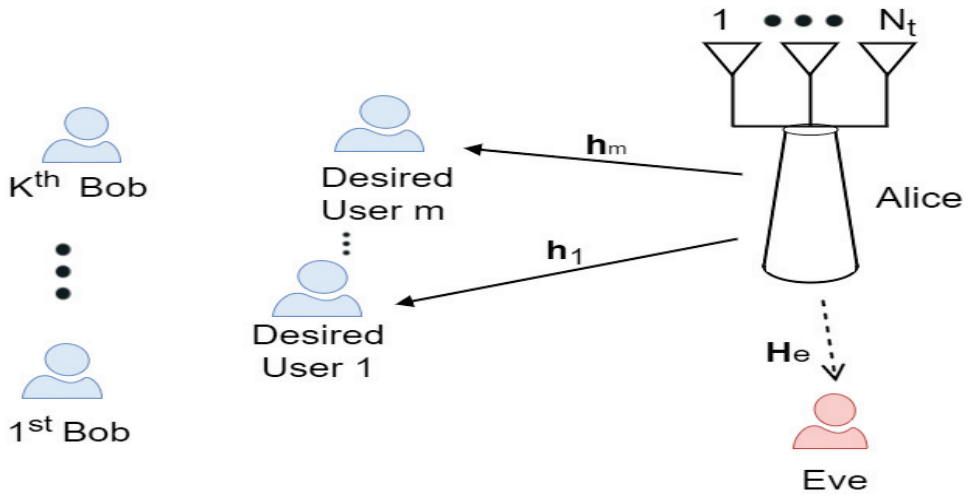

Figure 4.11. A system model that consists a multi-antenna transmitter, K legitimate receivers with single antenna and an eavesdropper with multiple-antenna

Transmitted signal is masked with artificial noise and it may be expressed as

$$\mathbf{x} = \hat{\mathbf{W}}\mathbf{s} + \hat{\mathbf{Q}}\mathbf{a}, \tag{4.12}$$

where $\hat{\mathbf{Q}}$ is the quantized orthogonal basis of the null space of $\mathbf{H}(\mathbb{M})$ and $\mathbf{a}$ is the artificial noise vector.

In order to guarantee the existence of matrix $\hat{\mathbf{Q}}$, the number of transmitter antenna N_t, must be higher than number of selected user M. Further, to prevent eavesdropper to eliminate artificial noise $N_t - M \geq N_e$ must be satisfied. Thus, we select number of M legitimate users

to send confidential messages simultaneously that satisfies above conditions.

Based on semi orthogonal user selection the M legitimate users at the transmitter, the received signal at the m^{th} legitimate user is written as,

$$\hat{y}_m = \mathbf{h}_m^H \hat{\mathbf{w}}_m s_m + \sum_{j=1, j\neq m}^{M} \mathbf{h}_m^H \hat{\mathbf{w}}_j s_j + \mathbf{h}_m^H \hat{\mathbf{Q}} \mathbf{a} + n_m. \tag{4.13}$$

We assume worst-case scenario in which eavesdropper can cancel interference from other users. Then, the received signal belonging to the m^{th} legitimate user at the eavesdropper is expressed by

$$\mathbf{y}_{e_m} = \mathbf{H}_E \hat{\mathbf{w}}_m s_m + \mathbf{H}_E \hat{\mathbf{Q}} \mathbf{a} + \mathbf{n}_e, \tag{4.14}$$

Thus, achievable secrecy sum-rate

$$R = \sum_{m=1}^{M} \left(\mathbb{E}\left\{ \log_2(1 + \hat{\gamma}_m) \right\} - \mathbb{E}\left\{ \log_2(1 + \hat{\gamma}_{e_m}) \right\} \right)^+, \tag{4.15}$$

where $\hat{\gamma}_m$ and $\hat{\gamma}_{e_m}$ correspond to SINR values at legitimate user and eavesdropper for m^{th} message respectively. The m^{th} legitimate user's SINR can be written as,

$$\hat{\gamma}_m = \frac{p_s |\mathbf{h}_m^\dagger \hat{\mathbf{w}}_m|^2}{p_s \sum_{j=1, j\neq m}^{M} |\mathbf{h}_m^\dagger \hat{\mathbf{w}}_j|^2 + p_a |\mathbf{h}_m^\dagger \hat{\mathbf{Q}}|^2 + \sigma^2}, \quad m = 1, 2, \ldots, M \tag{4.16}$$

Then, the SINR at eavesdropper can be expressed as,

$$\hat{\gamma}_{e_m} = p_s (\mathbf{H}_E \hat{\mathbf{w}}_m)^\dagger (\sigma_e^2 \mathbf{I} + p_a (\mathbf{H}_E \hat{\mathbf{Q}})(\mathbf{H}_E \hat{\mathbf{Q}})^\dagger)^{-1} (\mathbf{H}_E \hat{\mathbf{w}}_m), \quad m = 1, 2, \ldots, M \tag{4.17}$$

where total transmit power is denoted as P which is equal to sum of information and AN signal powers ($p_s + p_a$), where $p_s = \frac{\alpha P}{M}$ and $p_a = \frac{(1-\alpha)P}{N_t - M}$ respectively. Power allocation between informtion and AN signals affects the secrecy capacity. According to availability of particular channel state informations at transmitter (perfect or quantized), the value of α parameter should be chosen wisely as it provides the optimum secrecy capacity.

The purpose of artificial noise is to disturb any possible eavesdropper reception by beamforming noise in all directions except from legitimate users' channel directions. However, the lack of perfect CSI at transmitter causes a noise leakage on legitimate users' channels and it degrades achievable secrecy rate. Therefore, we use Rotated Codebook based on the semi orthogonal selection criteria to reduce the quantization errors in order to prevent noise leakage and inter user interference as described in Section 4.2.

4.5. Performance Evaluations

We illustrate the simulation results for $N_t = 4$ transmit antennas at Alice and $N_e = 2$ antennas at Eve unless stated otherwise. The pair of $(\gamma_{th}, \epsilon_{th})$ for $\mathcal{T}_3$ criterion is calculated to have an average number of users in the cell $\bar{K} = 4$.Then, the pairs are chosen as $(\gamma_{th}, \epsilon_{th}) = [(0.45, 0.60), (0.322, 0.60), (0.293, 0.60), (0.272, 0.60)]$. Only the legitimate users that satisfy these thresholds are fed back their B bits corresponding to the codebook index of their quantized CDI to Alice. Exploiting the feedback information, Alice schedules the M legitimate users by performing ZFBF to reduce inter-user interference.

The effect of power allocation parameter α for the quantized case with $B = 8$ is examined in Figure 4.12 at SNR=10dB. As seen from the figure, $\alpha = 0.6$ is the optimum value for this simulation. In Figure 4.13, we compare the secrecy capacity for the system that performs semi-orthogonal selection with Rotated codebook and full feedback system with Lloyd codebook for number of active users with AN having the optimal power allocation based on Figure 4.12. The performance results show that the proposed solution for multiuser MISO system provides much better secrecy capacity performance than full feedback Lloyd codebook used system while requiring much less overhead through feedback link.

The comparison of full feedback and $\mathcal{T}_3$ with rotated and Lloyd codebooks is depicted for SNR in Figure 4.14. Increasing SNR can degrade the secrecy rate for Lloyd codebook used systems, since AN leakage is severe and it increases with SNR. In Figure 4.15, we compare performance of Rotated codebook for different number of bits. Also, in In Figure 4.16, we compare performance of Lloyd codebook for different number of bits. As can be seen from these two figure, Rotated codebook has higher performance.

In Figure 4.16, we compare the secrecy capacity for the system that performs semi-orthogonal selection having Rotated codebook and the system that schedules only one legitimate user with AN having the optimal power allocation based on Figure 4.12. The performance results are shown that the proposed solution for multiuser MISO system provides much better secrecy capacity performance than single user MISO system while requiring much less feedback bits in Figure 4.17 .

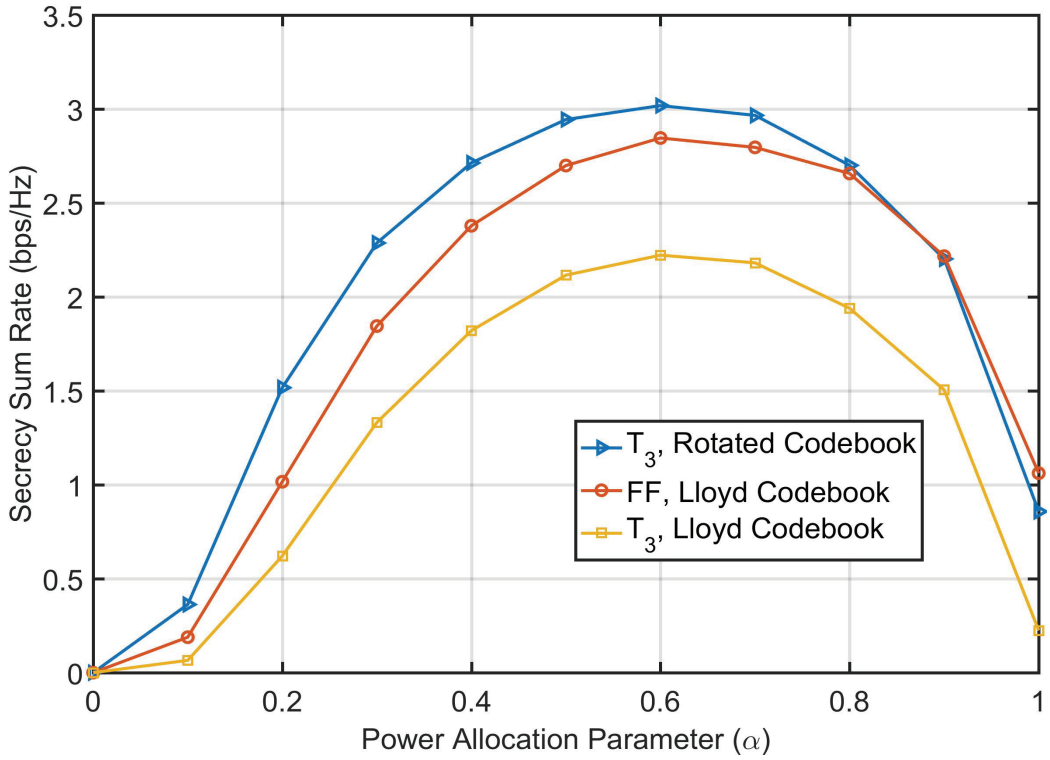

Figure 4.12. The power allocation parameter for full feedback and $\mathcal{T}_3$ criterion at $B = 8$ for different codebooks at SNR= 10dB.

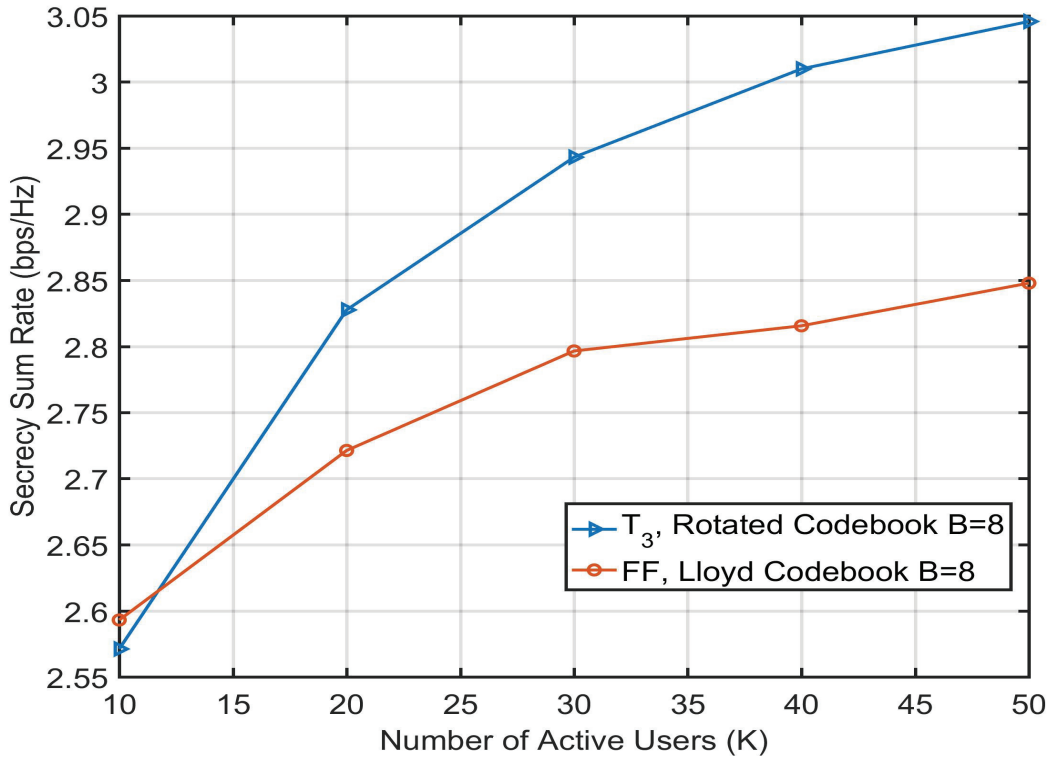

Figure 4.13. The comparison of full feedback and $\mathcal{T}_3$ criterion at $B = 8$ and SNR=10 dB for different codebooks and different number of users values where $\alpha = 0.6$

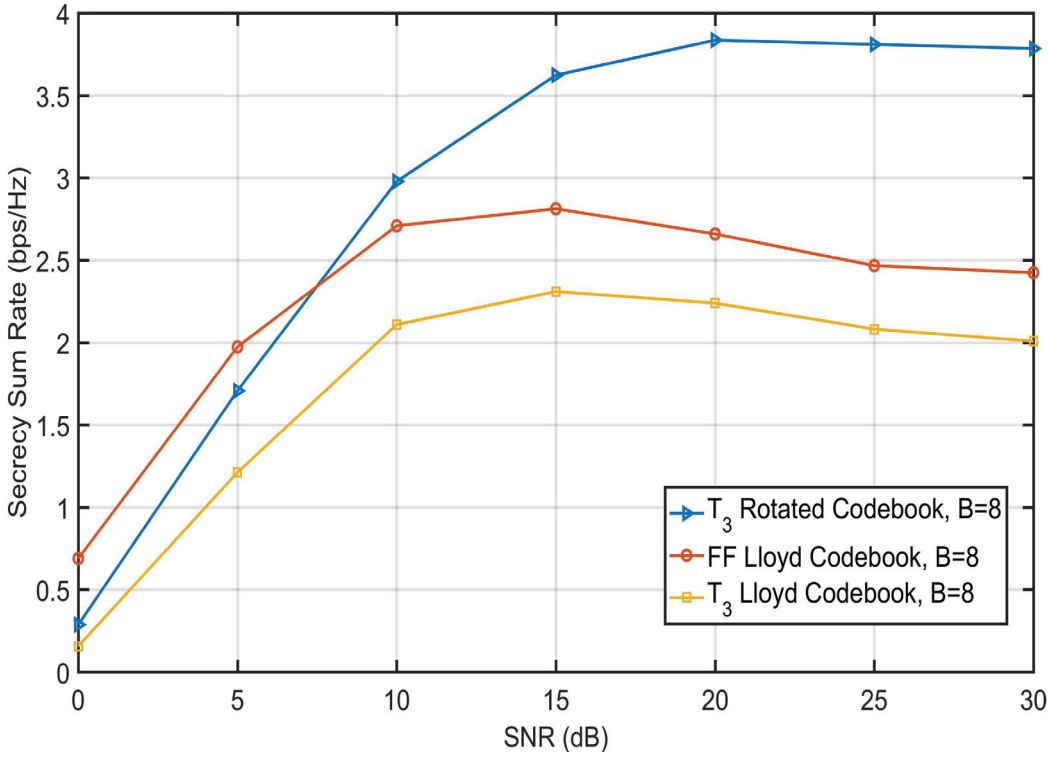

Figure 4.14. The comparison of full feedback and $\mathcal{T}_3$ criterion at $B = 8$ for different codebooks and SNR values where $\alpha = 0.6$, $K = 50$

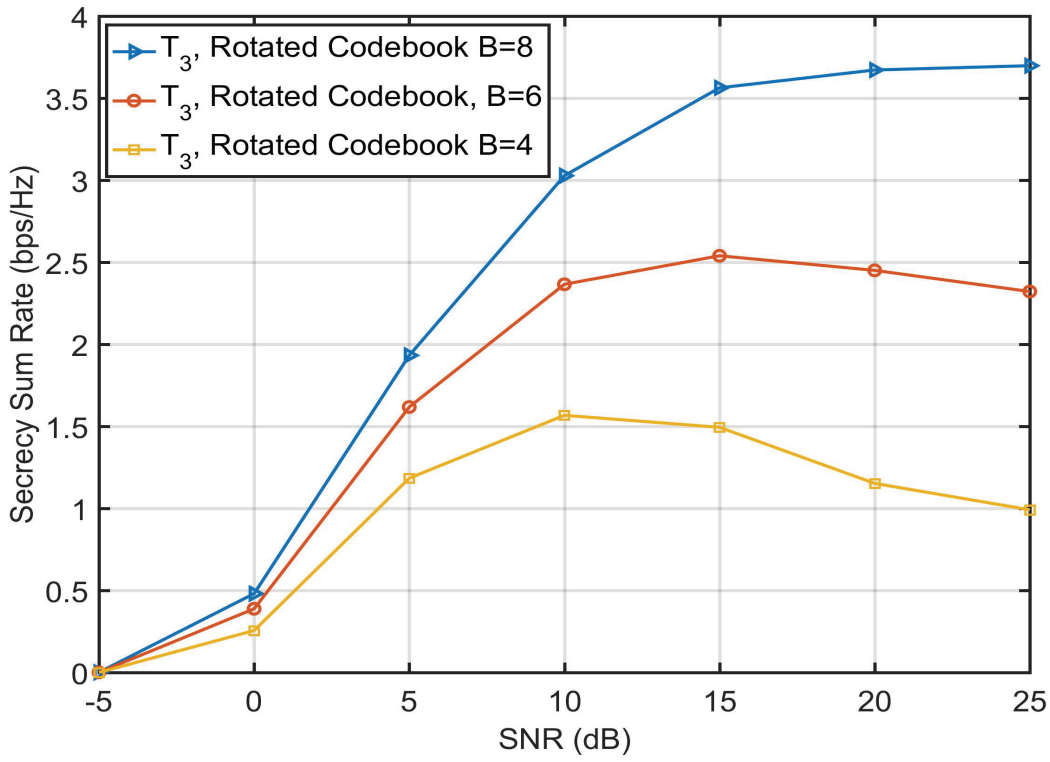

Figure 4.15. The comparison of $\mathcal{T}_3$ criterion for different number of bits where $K = 50$

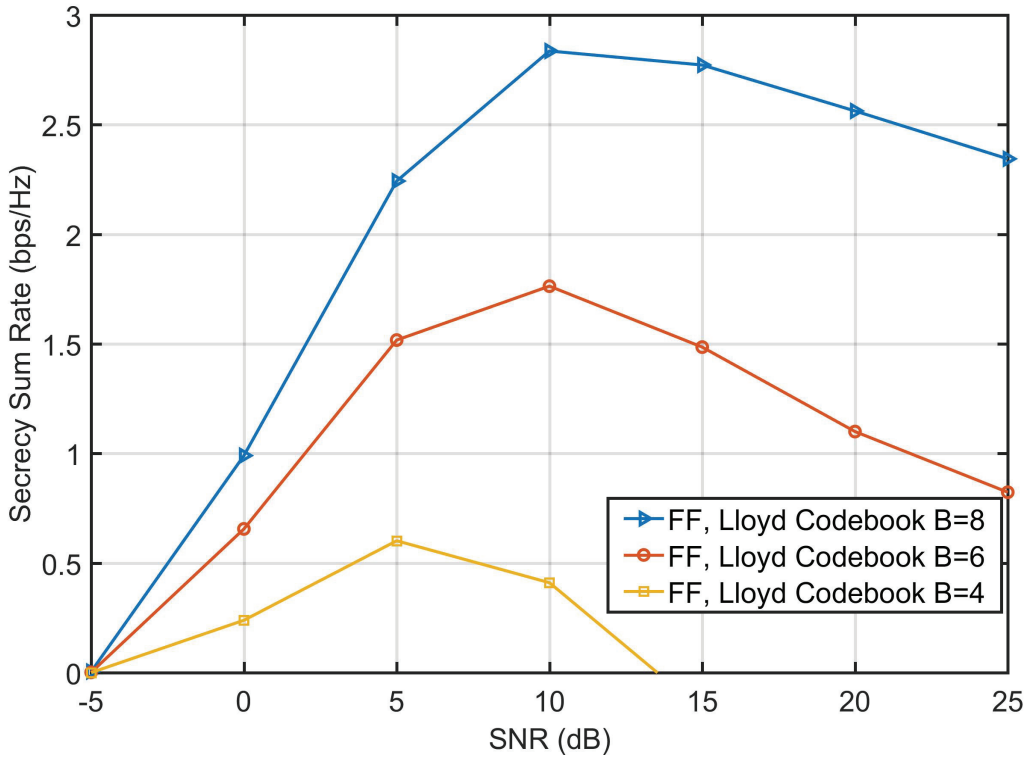

Figure 4.16. The comparison of full feedback criterion for different number of bits where $K = 50$

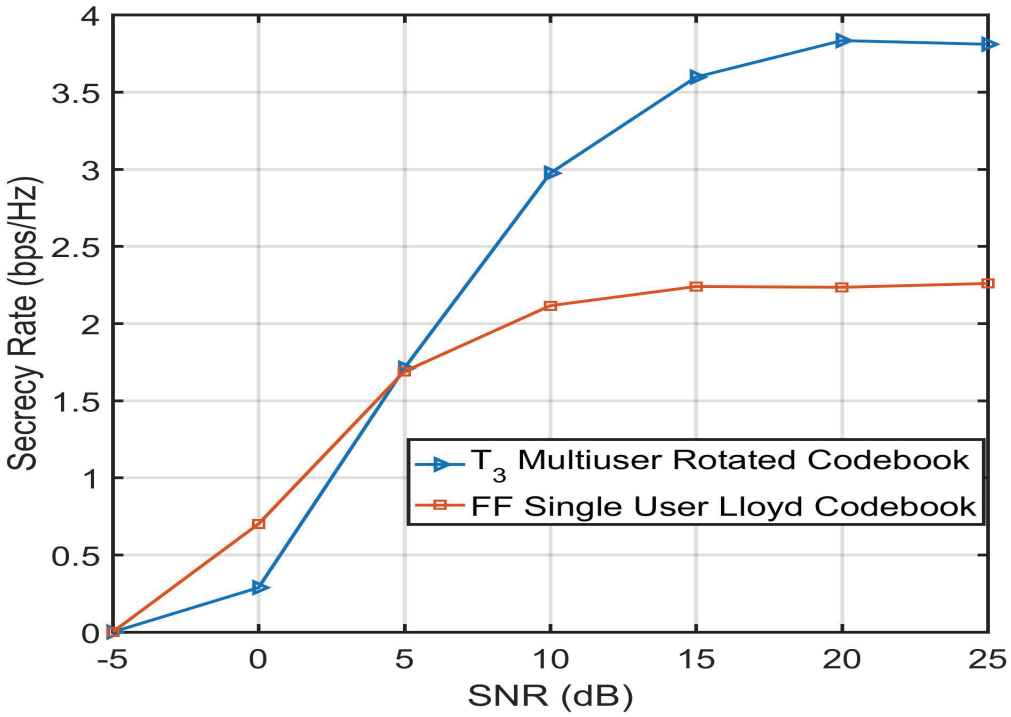

Figure 4.17. The comparison of $\mathcal{T}_3$ criterion for multiuser MISOME and full feedback for single user MISOME system where $K = 50$ and $\alpha = 0.6$

CHAPTER 5

CONCLUSION

In this thesis, we have studied PHY security based on multiple antenna technologies. Since the wireless transmission is vulnerable to interception of unauthorized receivers, the main focus of this thesis is to develop PHY security enhancement mechanisms especially in multiuser MIMO systems with a limited feedback link.

Firstly, we considered the secure single user scheduled MISO systems with a multiple antenna external eavesdropper for two different channel models. The information signal is masked with artificially generated noise to disrupt reception of any possible eavesdropper that maliciously try to attain it. Our goal for the single user scheduled MISO secure wireless communications is to mitigate noise leakage on user's channels while reaching multiplexing gain. Additionally, one of our focus is to reduce the feedback load using appropriate transmit beamforming mechanisms. In order to increase secrecy rate and overcome the noise leakage problem, a large number of quantization bits should be used. As the number of employed antennas grows, the total feedback load even become larger. With employing the norm based user selection at receiver side, namely $\mathcal{T}_1$, this feedback load is reduced. Thus, using lower number of feedback bits secure communication can be achieved.

The first system model is examined the secrecy rate performance of quasi-static fading channel. More specifically, we are interested in the case which legitimate users also receive AN since, in general only quantized CDI is available at the transmitter due to rate limitations on the feedback channel. In the second system model, we considered the temporally correlated fading channels and a transmit beamforming scheme that uses differential codebooks. The differential codebook are employed in order to track channel variations successfully and enable secure communications in fading temporally correlated fading channels.

On the other hand, increasing number of active users also increases the overhead in multiuser communications. We aimed to construct receiver side user selection mechanisms with rotated codebook design to achieve secure multiuser communcations. We considered two different secure multiuser scheduled MISO systems with passive eavesdroppers that equipped with various numbers of antennas. The semi-orthogonal user selection at receiver side, namely $\mathcal{T}_3$ is employed. We provided a transmission scheme that utilizes inter-user interference as a jamming method. The system model includes a single antenna eavesdropper with unknown CSI at transmitter. Then we present a system model that consists an multiple antenna eavesdropper corresponds to an alliance of geographically dispersed but perfectly cooperating sin-

gle antenna eavesdroppers. In that case artificial noise beamforming employed along with rotated codebook and receiver side user selection instead of inter-user interference jamming.

Our approaches are capable of enhancing the security of wireless communications by selecting the users with favorable channel conditions and quantizing CDI by the rotated codebook. Simulation results demonstrate the feasibility of these PHY security mechanisms by examining the achievable secrecy rates for all system models.

Overall, PHY security techniques can provide an achievable secrecy rate which is critical for many applications. These techniques can be viewed as integral part of the cross-layer security approaches. For instance, the existing cryptographic methods can be implemented together with PHY security schemes. In the near future, demands that need to be addressed are increased capacity, improved data rate, decreased latency, and better quality of service. In order to meet these demands, drastic improvements need to be made in current network architecture. Some of the emerging technologies that are considered as a probable solutions are heterogeneous networks, mm-wave systems, ultra-dense networks, device to device communications. As future work, the methods that are examined in this thesis can be extended to this systems since secrecy is a very crucial issue in these emerging wireless technologies.

REFERENCES

Allen Gersho, R. M. G. (1991). *Vector Quantization and Signal Compression*. Springer.

Bagherikaram, G., A. S. Motahari, and A. K. Khandani (2013, May). The secrecy capacity region of the gaussian mimo broadcast channel. *IEEE Transactions on Information Theory 59*(5), 2673–2682.

Carleial, A. and M. Hellman (1977, May). A note on wyner's wiretap channel (corresp.). *IEEE Transactions on Information Theory 23*(3), 387–390.

Chen, J., X. Chen, W. H. Gerstacker, and D. W. K. Ng (2016, Aug). Resource allocation for a massive mimo relay aided secure communication. *IEEE Transactions on Information Forensics and Security 11*(8), 1700–1711.

Chia, Y. K. and A. E. Gamal (2012, May). Three-receiver broadcast channels with common and confidential messages. *IEEE Transactions on Information Theory 58*(5), 2748–2765.

Choi, J., B. Clerckx, N. Lee, and G. Kim (2012, February). A new design of polar-cap differential codebook for temporally/spatially correlated miso channels. *IEEE Transactions on Wireless Communications 11*(2), 703–711.

Cover, T. (1972, Jan). Broadcast channels. *IEEE Transactions on Information Theory 18*(1), 2–14.

Csiszar, I. and J. Korner (1978, May). Broadcast channels with confidential messages. *IEEE Transactions on Information Theory 24*(3), 339–348.

Deng, H., H. M. Wang, J. Yuan, W. Wang, and Q. Yin (2016, Aug). Secure communication in uplink transmissions: User selection and multiuser secrecy gain. *IEEE Transactions on Communications 64*(8), 3492–3506.

Dong, L., Z. Han, A. P. Petropulu, and H. V. Poor (2009, Aug). Cooperative jamming for wireless physical layer security. In *2009 IEEE/SP 15th Workshop on Statistical Signal Processing*, pp. 417–420.

Dong, L., Z. Han, A. P. Petropulu, and H. V. Poor (2010, March). Improving wireless physi-

cal layer security via cooperating relays. *IEEE Transactions on Signal Processing 58*(3), 1875–1888.

Du, C., X. Chen, and L. Lei (2015, Oct). Energy-efficient power allocation for secure communications in wireless powered massive mimo relaying systems. In *2015 International Conference on Wireless Communications Signal Processing (WCSP)*, pp. 1–6.

Fakoorian, S. A. A. and A. L. Swindlehurst (2011, Dec). Dirty paper coding versus linear gsvd-based precoding in mimo broadcast channel with confidential messages. In *2011 IEEE Global Telecommunications Conference - GLOBECOM 2011*, pp. 1–5.

Fakoorian, S. A. A. and A. L. Swindlehurst (2012, July). Optimal power allocation for gsvd-based beamforming in the mimo gaussian wiretap channel. In *2012 IEEE International Symposium on Information Theory Proceedings*, pp. 2321–2325.

Fakoorian, S. A. A. and A. L. Swindlehurst (2013, September). On the optimality of linear precoding for secrecy in the mimo broadcast channel. *IEEE Journal on Selected Areas in Communications 31*(9), 1701–1713.

Geraci, G., M. Egan, J. Yuan, A. Razi, and I. B. Collings (2012, November). Secrecy sum-rates for multi-user mimo regularized channel inversion precoding. *IEEE Transactions on Communications 60*(11), 3472–3482.

Gerbracht, S., C. Scheunert, and E. A. Jorswieck (2012, April). Secrecy outage in miso systems with partial channel information. *IEEE Transactions on Information Forensics and Security 7*(2), 704–716.

Gesbert, D. and M. S. Alouini (2004, June). How much feedback is multi-user diversity really worth? In *2004 IEEE International Conference on Communications (IEEE Cat. No.04CH37577)*, Volume 1, pp. 234–238.

Goel, S. and R. Negi (2008, June). Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications 7*(6), 2180–2189.

Gopala, P. K., L. Lai, and H. E. Gamal (2008, Oct). On the secrecy capacity of fading channels. *IEEE Transactions on Information Theory 54*(10), 4687–4698.

Hafez, M. and H. Arslan (2015, June). On directional modulation: An analysis of transmis-

sion scheme with multiple directions. In *2015 IEEE International Conference on Communication Workshop (ICCW)*, pp. 459–463.

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

Huang, J. and A. L. Swindlehurst (2011, May). Cooperation strategies for secrecy in mimo relay networks with unknown eavesdropper csi. In *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 3424–3427.

Jindal, N. (2006, Nov). Mimo broadcast channels with finite-rate feedback. *IEEE Transactions on Information Theory 52*(11), 5045–5060.

Khisti, A., A. Tchamkerten, and G. W. Wornell (2008, June). Secure broadcasting over fading channels. *IEEE Transactions on Information Theory 54*(6), 2453–2469.

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

Krikidis, I. and B. Ottersten (2013, Feb). Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling. *IEEE Signal Processing Letters 20*(2), 141–144.

Lai, L. and H. E. Gamal (2008, Sept). The relay eavesdropper channel: Cooperation for secrecy. *IEEE Transactions on Information Theory 54*(9), 4005–4019.

Leung-Yan-Cheong, S. and M. Hellman (1978, Jul). The gaussian wire-tap channel. *IEEE Transactions on Information Theory 24*(4), 451–456.

Li, N., X. Tao, H. Chen, and H. Wu (2016, April). Secrecy outage probability for the multiuser downlink with several curious users. In *2016 IEEE Wireless Communications and Networking Conference*, pp. 1–5.

Li, N., X. Tao, H. Wu, J. Xu, and Q. Cui (2016, Sept). Large-system analysis of artificial-noise-assisted communication in the multiuser downlink: Ergodic secrecy sum rate and optimal power allocation. *IEEE Transactions on Vehicular Technology 65*(9), 7036–7050.

Li, Q., M. Hong, H. T. Wai, Y. F. Liu, W. K. Ma, and Z. Q. Luo (2013, September). Transmit

solutions for mimo wiretap channels using alternating optimization. *IEEE Journal on Selected Areas in Communications 31*(9), 1714–1727.

Li, Q. and W. K. Ma (2011, Aug). Optimal and robust transmit designs for miso channel secrecy by semidefinite programming. *IEEE Transactions on Signal Processing 59*(8), 3799–3812.

Liang, Y., H. V. Poor, and S. Shamai (2008, June). Secure communication over fading channels. *IEEE Transactions on Information Theory 54*(6), 2470–2492.

Liao, W. C., T. H. Chang, W. K. Ma, and C. Y. Chi (2010, March). Joint transmit beamforming and artificial noise design for qos discrimination inwireless downlink. In *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 2562–2565.

Lin, C. H., S. H. Tsai, and Y. P. Lin (2014, May). Secure transmission using mimo precoding. *IEEE Transactions on Information Forensics and Security 9*(5), 801–813.

Lin, S. C., T. H. Chang, Y. L. Liang, Y. W. P. Hong, and C. Y. Chi (2011, March). On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem. *IEEE Transactions on Wireless Communications 10*(3), 901–915.

Liu, R. and H. V. Poor (2009, March). Secrecy capacity region of a multiple-antenna gaussian broadcast channel with confidential messages. *IEEE Transactions on Information Theory 55*(3), 1235–1249.

Liu, T. and S. Shamai (2009, June). A note on the secrecy capacity of the multiple-antenna wiretap channel. *IEEE Transactions on Information Theory 55*(6), 2547–2553.

Liu, X., F. Gao, G. Wang, and X. Wang (2014, January). Joint beamforming and user selection in multicast downlink channel under secrecy-outage constraint. *IEEE Communications Letters 18*(1), 82–85.

Love, D. J., R. W. Heath, and T. Strohmer (2003, May). Grassmannian beamforming for multiple-input multiple-output wireless systems. In *Communications, 2003. ICC '03. IEEE International Conference on*, Volume 4, pp. 2618–2622 vol.4.

Ly, H. D., T. Liu, and Y. Liang (2010, Nov). Multiple-input multiple-output gaussian broadcast channels with common and confidential messages. *IEEE Transactions on Information*

Theory 56(11), 5477–5487.

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

Mukherjee, A. and A. L. Swindlehurst (2009a, Nov). User selection in multiuser mimo systems with secrecy considerations. In *2009 Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers*, pp. 1479–1482.

Mukherjee, A. and A. L. Swindlehurst (2009b, Sept). Utility of beamforming strategies for secrecy in multiuser mimo wiretap channels. In *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 1134–1141.

Mukkavilli, K. K., A. Sabharwal, E. Erkip, and B. Aazhang (2003, Oct). On beamforming with finite rate feedback in multiple-antenna systems. *IEEE Transactions on Information Theory 49*(10), 2562–2579.

Narula, A., M. J. Lopez, M. D. Trott, and G. W. Wornell (1998, Oct). Efficient use of side information in multiple-antenna data transmission over fading channels. *IEEE Journal on Selected Areas in Communications 16*(8), 1423–1436.

Negi, R. and S. Goel (2005, Sept). Secret communication using artificial noise. In *VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005.*, Volume 3, pp. 1906–1910.

Negro, F., S. P. Shenoy, I. Ghauri, and D. T. M. Slock (2010, Sept). Weighted sum rate maximization in the mimo interference channel. In *21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 684–689.

Oggier, F. and B. Hassibi (2011, Aug). The secrecy capacity of the mimo wiretap channel. *IEEE Transactions on Information Theory 57*(8), 4961–4972.

Ozbek, B. and D. Le Ruyet (2014). In *Feedback Strategies for Wireless Communication*. Springer.

Ozbek, B., O. Ozdogan, and G. K. Kurt (2016, Sept). Secure multiuser miso communication systems with quantized feedback. In *2016 IEEE 27th Annual International Symposium on*

Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, pp. 1–6.

Ozbek, B., O. Ozdogan, and G. K. Kurt (2017). Secure multiuser miso communication systems with limited feedback link. In *Submitted to: Annals of Telecommunications Journal, Springer*.

Ozdogan, O., B. Ozbek, and G. K. Kurt (2016, May). Performance of secure multiuser miso systems with threshold based user selection. In *2016 24th Signal Processing and Communication Application Conference (SIU), Zonguldak*, pp. 721–724.

Ozdogan, O., B. Ozbek, and G. K. Kurt (2017a, May). Performance of limited feedback secure miso systems in temporally correlated channels. In *2017 25th Signal Processing and Communications Applications Conference (SIU), Antalya*, pp. 1–4.

Ozdogan, O., B. Ozbek, and G. K. Kurt (2017b). Secure multiuser miso communication systems with imperfect channel state information. In *Submitted to: Transactions on Emerging Telecommunications Technologies Journal, Wiley*.

Peng, Z., J. Zhu, W. Xu, H. Zhang, and C. Zhao (2014, Dec). Impact of estimated csi quantization on secrecy rate loss in pilot-aided mimo systems. In *2014 IEEE Globecom Workshops (GC Wkshps)*, pp. 1326–1331.

Roh, J. C. and B. D. Rao (2006, March). Transmit beamforming in multiple-antenna systems with finite rate feedback: a vq-based approach. *IEEE Transactions on Information Theory 52*(3), 1101–1112.

Schneier, B. (1996). Applied cryptography – protocols, algorithms, and source code in c.

Schneier, B. (1998, Sep). Cryptographic design vulnerabilities. *Computer 31*(9), 29–33.

Shafiee, S., N. Liu, and S. Ulukus (2009, Sept). Towards the secrecy capacity of the gaussian mimo wire-tap channel: The 2-2-1 channel. *IEEE Transactions on Information Theory 55*(9), 4033–4039.

Shafiee, S. and S. Ulukus (2007, June). Achievable rates in gaussian miso channels with secrecy constraints. In *2007 IEEE International Symposium on Information Theory*, pp. 2466–2470.

Shannon, C. E. (1949, Oct). Communication theory of secrecy systems. *The Bell System Technical Journal 28*(4), 656–715.

Sharif, M. and B. Hassibi (2005, Feb). On the capacity of mimo broadcast channels with partial side information. *IEEE Transactions on Information Theory 51*(2), 506–522.

Valliappan, N., A. Lozano, and R. W. Heath (2013, August). Antenna subset modulation for secure millimeter-wave wireless communication. *IEEE Transactions on Communications 61*(8), 3231–3245.

Wang, H. M., C. Wang, and D. W. K. Ng (2015, Dec). Artificial noise assisted secure transmission under training and feedback. *IEEE Transactions on Signal Processing 63*(23), 6285–6298.

Weingarten, H., Y. Steinberg, and S. S. Shamai (2006, Sept). The capacity region of the gaussian multiple-input multiple-output broadcast channel. *IEEE Transactions on Information Theory 52*(9), 3936–3964.

Wyner, A. D. (1975, Oct). The wire-tap channel. *The Bell System Technical Journal 54*(8), 1355–1387.

Wyner, A. D. (1994, Nov). Shannon-theoretic approach to a gaussian cellular multiple-access channel. *IEEE Transactions on Information Theory 40*(6), 1713–1727.

Xia, P. and G. B. Giannakis (2006, May). Design and analysis of transmit-beamforming based on limited-rate feedback. *IEEE Transactions on Signal Processing 54*(5), 1853–1863.

Xiong, J., K. K. Wong, D. Ma, and J. Wei (2012, September). A closed-form power allocation for minimizing secrecy outage probability for miso wiretap channels via masked beamforming. *IEEE Communications Letters 16*(9), 1496–1499.

Yamamoto, H. (1989, May). Coding theorem for secret sharing communication systems with two noisy channels. *IEEE Transactions on Information Theory 35*(3), 572–578.

Yamamoto, H. (1991, May). A coding theorem for secret sharing communication systems with two gaussian wiretap channels. *IEEE Transactions on Information Theory 37*(3), 634–638.

Yanase, M. and T. Ohtsuki (2010, Aug). User selection scheme with secrecy capacity between other users in mimo downlink systems. In *2010 IEEE International Conference on Wireless Information Technology and Systems*, pp. 1–4.

Yang, J., I. M. Kim, and D. I. Kim (2013, June). Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers. *IEEE Transactions on Wireless Communications 12*(6), 2840–2852.

Yang, Y., W. Wang, H. Zhao, and L. Zhao (2012, Aug). Transmitter beamforming and artificial noise with delayed feedback: Secrecy rate and power allocation. *Journal of Communications and Networks 14*(4), 374–384.

Yeung, C. K. A. and D. J. Love (2005, Oct). Performance analysis of random vector quantization limited feedback beamforming. In *Conference Record of the Thirty-Ninth Asilomar Conference onSignals, Systems and Computers, 2005.*, pp. 408–412.

Yusuf, M. and H. Arslan (2015, Sept). Secure multi-user transmission using comp directional modulation. In *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, pp. 1–2.

Zhang, H., Y. Huang, S. Li, and L. Yang (2014, Sept). Energy-efficient precoder design for mimo wiretap channels. *IEEE Communications Letters 18*(9), 1559–1562.

Zhang, J., J. G. Andrews, and R. W. Heath (2008, Sept). Single-user mimo vs. multiuser mimo in the broadcast channel with csit constraints. In *2008 46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 309–314.

Zhang, X., M. R. McKay, X. Zhou, and R. W. Heath (2015, May). Artificial-noise-aided secure multi-antenna transmission with limited feedback. *IEEE Transactions on Wireless Communications 14*(5), 2742–2754.

Zheng, T. X. and H. M. Wang (2016, Oct). Optimal power allocation for artificial noise under imperfect csi against spatially random eavesdroppers. *IEEE Transactions on Vehicular Technology 65*(10), 8812–8817.

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

Zhu, J., R. Schober, and V. K. Bhargava (2016, July). Physical layer security for massive mimo systems impaired by phase noise. In *2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 1–5.