PHYSICAL LAYER SECURITY OVER FREQUENCY SELECTIVE FADING CHANNELS

A THESIS SUBMITTED TO

THE GRADUATE SCHOOL OF ENGINEERING AND SCIENCE

OF BILKENT UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR

THE DEGREE OF

MASTER OF SCIENCE

IN

ELECTRICAL AND ELECTRONICS ENGINEERING

By

Kadir Ayhan

January, 2016

PHYSICAL LAYER SECURITY OVER FREQUENCY SELECTIVE FADING CHANNELS
By Kadir Ayhan
January, 2016

We certify that we have read this thesis and that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Tolga M. Duman (Advisor)

Sinan Gezici

Bülent Tavlı

Approved for the Graduate School of Engineering and Science:

Levent Onural
Director of the Graduate School

ABSTRACT

PHYSICAL LAYER SECURITY OVER FREQUENCY SELECTIVE FADING CHANNELS

Kadir Ayhan
M.S. in Electrical and Electronics Engineering
Advisor: Tolga M. Duman
January, 2016

The inherent open nature of the transmission medium makes security a challenging issue in wireless networks. Physical layer security, which is an alternative or a complement to the cryptographic approaches, exploits the differences between the physical properties of different channels in order to provide secrecy. The idea is to ensure that the received signal at an eavesdropper is degraded compared to that of the legitimate receiver in some sense which guarantees that the confidential messages cannot be recovered by an unintended receiver. Over the last decade, various researchers have studied fundamental limits of physical layer security under different wiretap channel models, including Gaussian and fading channels, and with different assumptions on the transmitter's knowledge on the channel state information.

In this thesis, we study physical layer security over frequency selective fading channels modelling certain wireless links. Specifically, we investigate optimal and suboptimal power allocation schemes across frequencies with perfect and partial channel state information at the transmitter with the objective of providing secrecy. We demonstrate that frequency selectivity allows for positive secrecy rates even though the eavesdropper's channel is not a degraded version of the desired user's channel. We also analyse the impact of user mobility and the resulting time variations in the wireless medium on the achievable secrecy rates. Furthermore, we consider quantized channel state information at the transmitter and evaluate the secrecy rate loss due to limited feedback from the legitimate receiver to the transmitter. Our results reveal that the partial channel state information at the transmitter can still be helpful in providing positive secrecy rates.

Keywords: Physical layer security, frequency selective fading channels, power allocation, mobility, limited feedback channel.

ÖZET

FREKANS SEÇİCİ AZALAN KANALLLARDA FİZİKSEL KATMANDA GÜVENLİK

Kadir Ayhan
Elektrik ve Elektronik Mühendisliği, Yüksek Lisans
Tez Danışmanı: Tolga M. Duman
Ocak, 2016

Kablosuz ağlarda güvenlik, bu ortamın doğasından dolayı zorlu bir probleme dönüşür. Kriptografik yaklaşımların alternatifi ya da tamamlayıcısı olarak, fiziksel katmanda güvenlik, gizliliği sağlamak için farklı kanalların fiziksel özellikleri arasındaki farklılıkları kullanır. İstenen alıcının aldığı sinyale kıyasla istenmeyen alıcının aldığı sinyalin daha kötü olması, bazı durumlarda gizli mesajın istenmeyen alıcı tarafından çözülemeyeceğini garanti eder. Son on yılda, fiziksel katmanda güvenliğin temel sınırlarını anlamak için Gauss ve azalan kanalları içeren farklı kanal modelleri ile ilgili çalışmalar yapılmıştır.

Bu tezde, frekans seçici azalan kanallar üzerinde fiziksel katmanda güvenlik çalışılmıştır. Gizliliği sağlamak amacıyla farklı frekanslar arasında optimum ve optimum olmayan güç paylaştırma yöntemleri, göndericide istenen alıcının ve istenmeyen alıcının kanal bilgileri olduğu durumda ve sadece istenen alıcının kanal bilgisinin olduğu durumda incelenmiştir. İstenmeyen alıcının kanalı, istenen alıcının kanalından daha iyi olsa bile kanalların frekans seçiciliğinin yardımıyla sıfırdan büyük gizlilik kapasitesine erişebildiğini gösterdik. Ek olarak, kullanıcının hareketli olduğu durumlar üzerinde çalışıldı. Hareketlilikten dolayı kanalın zamanla değişmesinin, ulaşılabilir gizlilik kapasitesi üzerindeki etkisini analiz ettik. Ayrıca istenen alıcı ile gönderici arasındaki geribildirim kanalının kısıtlı olmasından dolayı istenen alıcı, kanal bilgisini kuantalanmış şekilde gönderir. Göndericide kuantalanmış kanal bilgisinin sebep olduğu gizlilik kapasitesindeki düşüşü inceledik. Elde ettiğimiz sonuçlar, sadece istenen alıcı kanalının − kuantalanmış versiyonunun gönderici tarafından bilinmesi durumunda bile − sıfırdan büyük gizlilik kapasitesinin elde edilebileceğini gösterdi.

Anahtar sözcükler: Fiziksel katmanda güvenlik, frekans seçici azalan kanallar, güç paylaştırma, hareketlilik, kısıtlı geri bildirim kanalı.

Acknowledgement

I would like to thank my advisor Prof. Dr. Tolga M. Duman for his supervision, suggestions and invaluable encouragement throughout the development of this thesis.

I would also like to thank the members of the thesis committee for reviewing the thesis.

I would like to thank Sina Rezaei Aghdam who helped me in the every part of my work.

I would like to thank Mehdi Dabirnia for his discussions and comments in my research. I also want to thank my friend Uğur İkinci for his supports during my research process.

I would like to thank staff at Meteksan Defense Industry Inc. for their support during my thesis.

I would also like to thank my wife, Banu and my parents for their endless support and encouragement throughout my graduate study.

Finally, I would like to thank The Scientific and Technological Research Council of Turkey (TÜBİTAK) for the financial support during my study. I am also grateful for being part of the TÜBİTAK project 113E223.

Contents

List of Figures

Chapter 1

Introduction

With the advent of more wireless capabilities in communication systems than ever, e.g., with the deployment of 3G, 4G, WIMAX and proposal of 5G etc., the issue of wireless security has become an increasingly important concern for communication systems designers. Due to the broadcast nature of wireless medium, wireless signals are available to anyone with a receiver with enough sensitivity, unlike the traditional wired or fiber optic media that require physical access to the communications path for signal interception. This makes wireless communications potentially more insecure and wireless security a challenging issue to deal with.

The problem of secrecy in communication systems has traditionally been tackled using cryptographic methods in the upper layers of the network. Though effective, these methods have been shown to have their own inherent difficulties, e.g., in secret key generation, distribution and management [1]. Hence, there have been a growing interest in the research community to study the use of other techniques in the physical layer to further enhance secrecy in wireless communication systems [2].

In physical layer security, the main idea derives from information theoretic approaches to transmit confidential messages securely to a legitimate receiver without using an encryption key by exploiting the differences between the channel to a legitimate receiver and the channel to an eavesdropper in order to benefit

the legitimate user. Secure transmission is enabled by using inherent randomness of the physical medium including noise and channel fluctuations due to its time-varying nature. The wireless medium provides plenty of additional randomness, for instance, fading and interference in addition to opportunities for vector communications via multiple antennas and cooperative communications through overheard signals and relaying [3].

Shannon introduced the concept of information-theoretic secrecy and provided a wiretap channel model where both a legitimate user and an eavesdropper observe the transmitted signal with no noise in [4]. In [5], Wyner considered a noisy wiretap channel and characterized the capacity-equivocation region for a scenario where the received signal at the eavesdropper is the degraded version of the signal received at the legitimate receiver. In [6], Csiszar and Korner studied the general, namely, not necessarily degraded, wiretap channel model and derived an expression for the secrecy capacity in the form of the difference between the mutual information expressions corresponding to the main channel and the eavesdropper's channel, to be maximized over the joint distribution of an auxiliary random variable and the channel input. This auxiliary random variable can be considered as performing pre-processing on the information.

In [7], Leung and Hellman generalized Wyner's results in [5] for discrete memoryless wiretap channels to the case of Gaussian wiretap channels and they proved that Gaussian signalling is optimal. Furthermore, they showed that the secrecy capacity is the difference between the capacities of the legitimate receiver and the eavesdropper if this difference is positive, and zero otherwise.

A long gap of about 30 years followed these initial papers until the research community has regained interest in physical layer security for wireless networks. As examples of recent contributions on the physical layer security over fading wiretap channels [3] and [8] can be given.

Barros and Rodrigues analysed the role of fading for secure communications in [9], where they assume that both channels experience quasi-static fading. Under a setup where the channel state information (CSI) of the eavesdropper is not available at the transmitter, they show that secure communications can be attained for the fraction of time when the main channel is stronger than the eavesdropper's channel. Bursty signaling is shown to mitigate the absence of information

about the eavesdropper's fading by Li, Yates, and Trappe [10] for independent and identically distributed (i.i.d.) Rayleigh fading. The secrecy capacity of block-fading channels for different cases in presence or absence of information about the eavesdropper's channels is established by Gopala, Lai, and El Gamal in [8], where the near optimality of bursty signalling is also proved for i.i.d. Rayleigh block-fading in the high-power regime.

Along with the various research contributions which have studied physical layer security for different scenarios, evaluation of secrecy performance over the frequency selective fading channels has also been of recent interest. In [11], a frequency selective channel is modelled as a multiple-input multiple-output (MIMO) Toeplitz matrix and a Vandermonde precoding scheme is proposed with the aid of perfect CSI at the transmitter (CSIT). Renna et al. [12] studies secrecy when orthogonal frequency division multiplexing (OFDM) is employed over a frequency selective channel. Another solution to secure communications over frequency selective fading channels is proposed in [13] where the authors argue that deep faded sub-channels of the legitimate receiver can be considered as the null space of frequency selective channels, and hence the transmitter can fill them with the noise in an effort to confuse the eavesdropper. Capacity degradation between the transmitter and the legitimate receiver is negligible, because the transmitter fills noise to already faded sub-channels, hence an enhanced secrecy performance can be obtained.

In this thesis, we further explore the physical layer security over frequency selective fading channels by deriving the optimal and suboptimal power allocation strategies with perfect and partial CSIT. We also analyze the impact of inter-carrier interference (ICI) on the achievable secrecy rates in time-varying multipath channels. A brief summary of the contributions and the outline of the thesis are provided in the next two subsections.

1.1 Summary of Contributions

In this thesis, optimal power allocation over frequency selective fading wiretap channels is studied when both the legitimate user's and the eavesdropper's channels are perfectly known at the transmitter. A low complexity algorithm is also proposed for the purpose of power allocation. Moreover, numerical examples are provided to analyze the effects of mobility on the secrecy rates. As a suboptimal but potentially effective strategy, when only the CSI of the legitimate receiver is available, the transmitter allocates power across different frequencies by using a water-filling algorithm. Closed form expression for secrecy rate is derived when this algorithm is utilized. Also, the performance of the water-filling power allocation scheme when only legitimate user's CSI is known at the transmitter is studied through several examples.

The thesis also considers partial CSI at the transmitter. We assume that there is a limited feedback channel from the legitimate receiver to the transmitter, and the legitimate receiver quantizes CSI of its own channel by using random vector quantization (RVQ). That is, the legitimate receiver selects a codeword in the common codebook, and then it sends a feedback message to the transmitter. Therefore, the transmitter knows the CSI of the legitimate receiver imperfectly and it utilizes a water-filling power allocation scheme with the aid of this imperfect information. Finally, numerical examples are provided to evaluate the effects of using the quantized version of the CSI at the transmitter on the achievable secrecy rates.

1.2 Thesis Outline

The thesis is organized as follows. Chapter 2 starts with a description of frequency selective fading channels. Then the principles of OFDM and the advantages of using OFDM over frequency selective fading channels are described. Furthermore, the secrecy capacity of additive white Gaussian noise (AWGN) and

fading channels are briefly reviewed. Lastly, a brief literature review on the physical layer security over frequency selective fading channels is given.

In Chapter 3, we explore the physical layer security problem over frequency selective fading channels. We investigate optimal and suboptimal power allocation schemes when the CSIs of both the eavesdropper and the legitimate receiver are available, and when only the CSI of the legitimate receiver is available at transmitter. We also examine the impact of mobility on the achievable secrecy rates in time-varying multipath channels.

In Chapter 4, we consider quantized CSI at the transmitter and evaluate the secrecy rate loss due to limited feedback from the legitimate receiver to the transmitter via a water-filling based solution and numerical examples.

Chapter 5 concludes the thesis and provides some possible directions for future research.

Chapter 2

Secure Transmission over Frequency Selective Fading Channels

This chapter provides some preliminaries required for the rest of the thesis. We start with a brief review of frequency selective fading channels and describe OFDM as a useful communication technique to combat frequency selectivity. After providing the formulation of the secrecy capacity over Gaussian channels, we study the fundamental limits of secure communications for block fading scenarios. Finally, we provide a review of the literature on the study of physical layer security over frequency selective channels, and conclude the chapter with a brief summary.

2.1 Frequency Selective Fading Channels

Due to a variety of phenomena, including refraction, reflection and scattering, transmitted signals over a wireless medium arrive at a receiver over multiple paths with different delays and strengths. Therefore, overall channel is modelled as a time-varying multi-path channel [14].

Multipath propagation in wireless channels results in frequency selectivity which arises in the broad-band wireless communications where the coherence bandwidth of the channel is smaller than the bandwidth of the transmitted signal. This is a valid model in practice because wideband transmission schemes are used for many modern wireless applications.

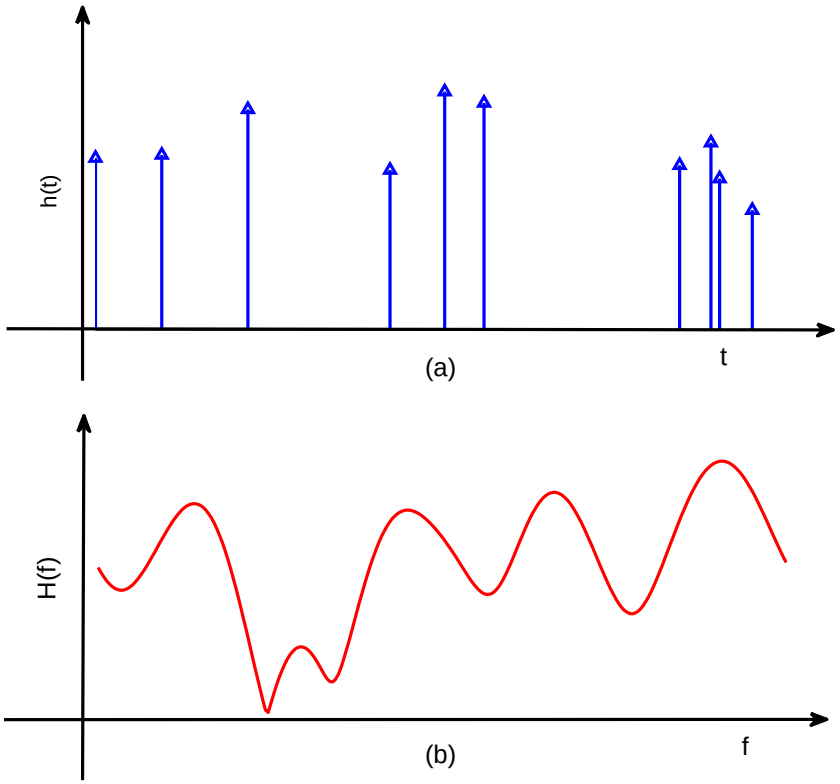

Figure 2.1: Illustration of multi-path effect. (a) Delays of signal caused by multi-path in time domain. (b) Frequency selective fading caused by multi-path effect.

For a multi-path channel assuming no time variations, the channel is modelled as a linear time invariant filter with an impulse response given by

$$h(t) = \sum_{l=0}^{L-1} \rho_l e^{j\theta_l} \delta(t - T_l) \tag{2.1}$$

where L represents the number of arriving signal copies at different delays (T_l's), and $\rho_l e^{j\theta_l}$ stands for the complex amplitude of l^{th} arriving signal component. This a widely accepted model for a frequency selective fading channel. The

corresponding frequency response can be obtained through a Fourier transform, i.e.,

$$H(f) = Fourier(h(t)) \tag{2.2}$$

$$= \int_{-\infty}^{\infty} h(t) e^{-j2\pi ft} dt \tag{2.3}$$

$$= \int_{-\infty}^{\infty} \left[\sum_{l=0}^{L-1} \rho_l e^{j\theta_l} \delta(t - T_l) \right] e^{-j2\pi ft} dt \tag{2.4}$$

$$= \sum_{l=0}^{L-1} \rho_l e^{j\theta_l} e^{-j2\pi fT_l}. \tag{2.5}$$

Figure 2.1-a illustrates a snapshot of impulse response of a frequency selective channel. From the equation above, it can be observed that for different frequencies, the magnitude of channel response in frequency domain varies which is depicted in Figure 2.1-b.

Time selective fading is another important characteristics of a wireless channel which arises as a result of relative mobility of the transmitter and receiver, or due to some other time-varying behavior in the propagation environment. In wireless communications, the fading channels generally exhibit both time-selectivity and frequency-selectivity and these characteristics are important elements in determining the wireless link quality. The frequency response given above should be considered as a snapshot of the behaviour of the channel with the understanding that it varies over time.

2.2 OFDM Principles

OFDM is a way of transmitting digital data by making use of multiple orthogonal sub-carriers. OFDM converts a frequency selective fading channel into a set of parallel frequency-flat sub-channels [15]. Block diagram of an OFDM system is depicted in Figure 2.2.

The incoming serial data with a high rate is initially turned into a parallel sequence with a low data rate. Each parallel sequence is modulated using an appropriate scheme, such as M-QAM or PSK, etc. Inverse fast Fourier transform (IFFT) block modulates these signals onto N orthogonal sub-carriers and

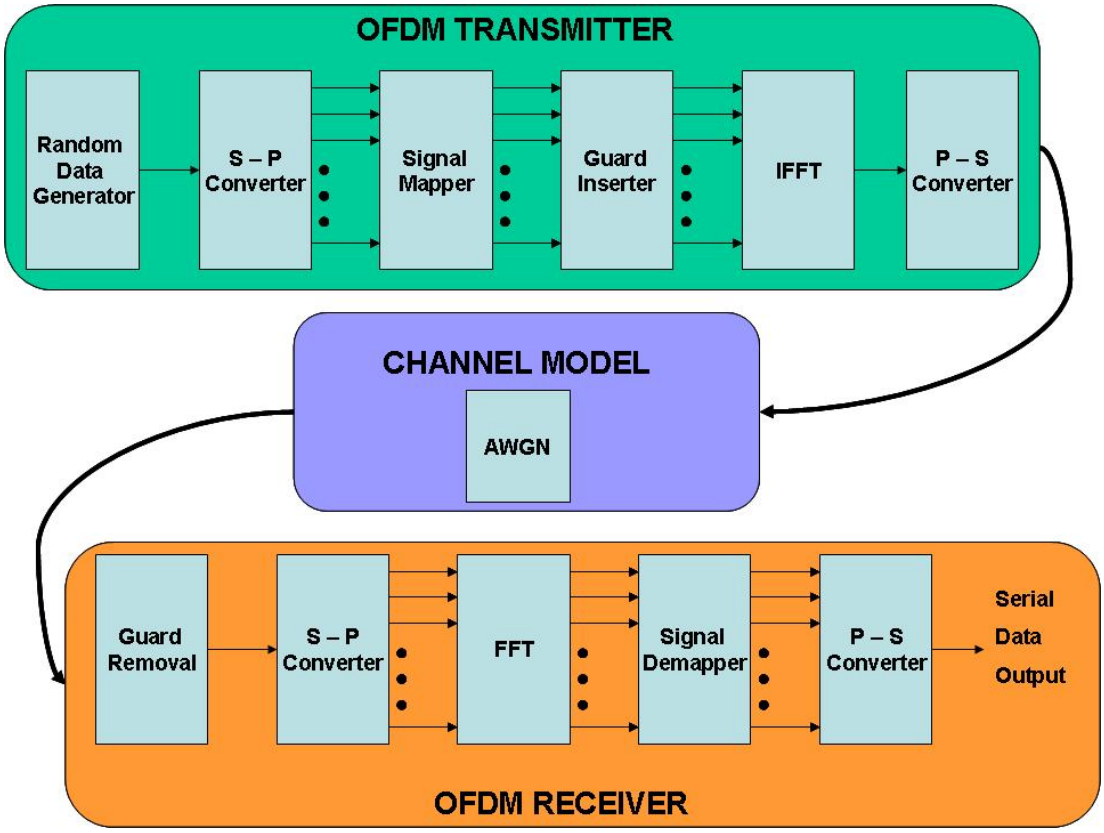

Figure 2.2: A block diagram of the OFDM system.

generates the time domain signals. Guard interval, e.g., in the form of a cyclic prefix, is added prior to the time domain signal generation in an effort to avoid the multi-path effects. The receiver removes the cyclic prefix, and it takes the fast Fourier of the samples of the incoming signal. The frequency domain signal is de-mapped by making use of the corresponding constellation mapping scheme, and hence the transmitted signal is recovered.

We utilize the OFDM scheme for two reasons. One of the reasons is that OFDM scheme is robust to frequency selective fading, due to the fact that it is insensitive to multi-path contained within the cyclic prefix. Accordingly, OFDM is employed in numerous applications and studying this scheme in the context of physical layer security is of interest. The second reason is that OFDM scheme gives us a practical way to study power allocation strategies across different frequencies. More specifically, OFDM divides the wideband signal into many narrowband sub-carriers, each exposed to flat fading rather than frequency selective

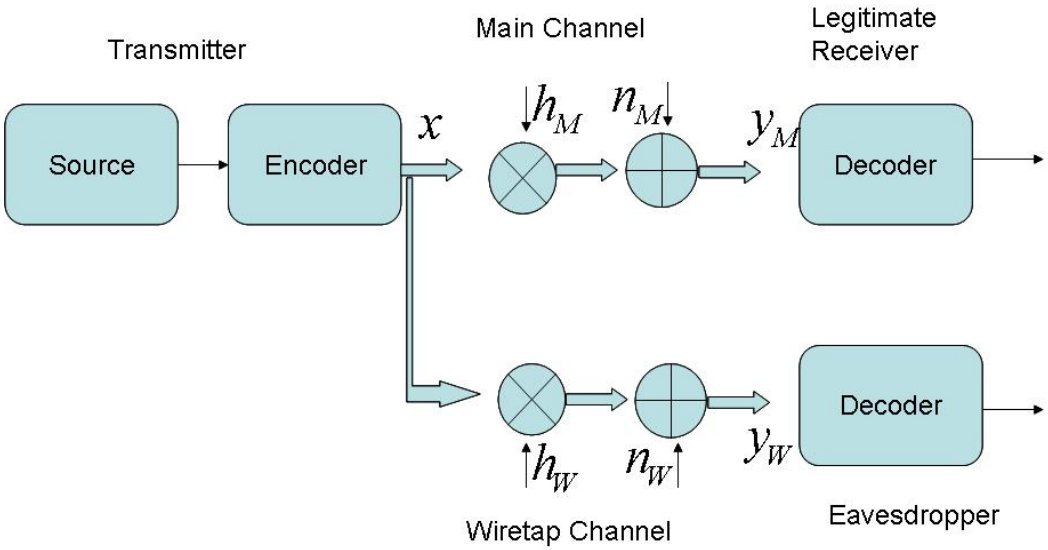

Figure 2.3: Communication system infrastructure with the existence of a wiretap channel.

fading. With the aid of this division, at each time instant, it is possible to find some sub-channels which are stronger in the direction of the legitimate receiver than in the direction of the eavesdropper. Accordingly a power allocation policy can be formulated which maximizes the quality difference between the received signals at the legitimate receiver and the eavesdropper. Such a policy gives rise to positive secrecy rates. The formulation of such achievable secrecy rates and resulting performance will be studied in the remainder of this thesis.

2.3 Secrecy Capaciy

We consider a wiretap channel as depicted in Figure 2.3. Consider a sequence of length k bits message w^k is encoded into a codeword of length n, x^n, to be transmitted through a flat (fading) channel. The signal received at the main user is modelled as

$$y_M = h_M x + n_M, \tag{2.6}$$

where h_M is the channel coefficient that also serves as the channel state information and n_M is a circularly symmetric Gaussian noise with zero-mean and σ_M^2

variance. The eavesdropper can overhear the signal that the transmitter sends where the signal received is described by

$$y_W = h_W x + n_W, \tag{2.7}$$

where h_W is the channel coefficient of the eavesdropper's channel and n_W is the circularly symmetric Gaussian noise with zero-mean and σ_W^2 variance. The transmitter is power limited in the sense that

$$\frac{1}{n}\sum_{i=1}^{n} E[|X|^2] \leq P_c, \tag{2.8}$$

where P_c is the maximum transmit signal power allowed.

AWGN Channels:

As a starting point, consider the main and the wiretap channels as AWGN channels, i.e., the channel gains are both set to $h_W = h_M = 1$. The power of noise in the main and the wire-tap channels are σ_M^2 and σ_W^2, respectively. The capacity of the main channel, which is achieved with Gaussian inputs, is obtained as [7]

$$C_M = log_2\left(1 + \frac{P_c}{\sigma_M^2}\right). \tag{2.9}$$

Likewise, the capacity of the eavesdropper's channel is

$$C_W = log_2\left(1 + \frac{P_c}{\sigma_W^2}\right). \tag{2.10}$$

Up until now, the capacity of both main channel and the eavesdropper's channel has been looked into. The secrecy capacity of the channel is defined in [9] as

$$C_S = C_M - C_W. \tag{2.11}$$

In other words, C_S is the capacity difference between the legitimate user's and eavesdropper's channels. This concept can be characterized in a way that if the maximum quantity of information transmitted in a legitimate channel is higher than the maximum quantity of information transmitted in a wire-tap channel,

the eavesdropper is likely to never receive enough information to break through the legitimate transmission.

It is important to remember that secure communication is attained in cases where $\sigma_W^2 > \sigma_M^2$ which accounts for a legitimate receiver who can receive more information than the eavesdropper. However, if $\sigma_W^2 < \sigma_M^2$, the transmission is unsecured, hence the secrecy capacity is zero. In other words, we have

$$C_S = \left[log_2 \left(1 + \frac{P_c}{\sigma_M^2} \right) - log_2 \left(1 + \frac{P_c}{\sigma_W^2} \right) \right]^+, \tag{2.12}$$

where $(x)^+ = \max\{x, 0\}$.

Fading Channels:

We now assume that both the main channel and the eavesdropper's channel experience block fading. Channel gains remain constant during each coherence interval. The fading process is ergodic with a bounded continuous distribution. Fading coefficients of both channels are independent of each other in any coherence interval. Furthermore, each coherence interval is large enough to allow for invoking random coding arguments. Under these assumptions, we investigate secrecy capacity under the condition that full CSI is known at transmitter, and secrecy rates when only main channel CSI is known at transmitter.

When the transmitter knows the CSI of the legitimate receiver and the wiretapper at the beginning of the each coherence interval, the secrecy capacity is given by [8]

$$C_s = \max_{P(h_m,h_w)} \int_0^\infty \int_0^\infty \left[log(1 + h_m P(h_m, h_w)) - log(1 + h_w P(h_m, h_w)) \right]^+ f(h_m) f(h_w) dh_m dh_w, \tag{2.13}$$

where h_m and h_w in the integral are the magnitude of channel gains of the legitimate receiver and the eavesdropper, respectively. $f(h_m)$ and $f(h_w)$ are probability density functions of h_m and h_w. $P(h_m, h_w)$ denotes the power allocation policy with perfect knowledge on h_m and h_w. The policy is required to satisfy the power constraint, i.e.,

$$E\left[P(h_m, h_w)\right] \leq P_c. \tag{2.14}$$

Since in the optimal scheme, the transmission is allowed only when $h_m > h_w$, the secrecy capacity can be written as

$$C_s = \max_{P(h_m,h_w)} \int_0^\infty \int_{h_w}^\infty [log(1 + h_m P(h_m, h_w)) - log(1 + h_w P(h_m, h_w))] \\ f(h_m) f(h_w) dh_m dh_w. \quad (2.15)$$

If we assume that the transmitter only knows the CSI of the main channel at the beginning of each coherence interval, and only a statistical knowledge of the eavesdropper's channel is available an achievable rate is given by [8];

$$R_s = \max_{P(h_m)} \int_0^\infty \int_{h_w}^\infty [log(1 + h_m P(h_m)) - log(1 + h_w P(h_m))] \\ f(h_m) f(h_w) dh_m dh_w, \quad (2.16)$$

where $P(h_m)$ is the power allocation policy with the aid of the main channel only, and it is selected such that $E[P(h_m)] \leq P_c$.

2.4 Physical Layer Security for Frequency Selective Fading Channels

An intriguing perspective dwelling on secrecy over frequency selective channels is proposed by Kobayashi and Debbah in [11]. In their study, the frequency selective channel is modelled as a multiple-input multiple-output Toeplitz matrix for both the active and passive eavesdropping scenarios. With the assumption of the perfect knowledge of the eavesdropper's CSI at the transmitter a Vandermonde precoding scheme is presented. This scheme offers a degree of freedom to transmit secret information depending on the number of available paths. For the most general case where the eavesdropper's channel is not available at the transmitter, one can make use of a mask beam-forming scheme with Vandermonde precoding in an effort to transmit artificial noise on the zeros of the legitimate channel for only jamming the eavesdropper. This scheme presents the drawback that both the intended receiver and the eavesdropped are forced to use the same receiver structure that corresponds to the description of parallel channel system. In the

case where the eavesdropper seizes on the information incorporated into the cyclic prefix, the system's security is put at risk. However, if this restriction is assumed, the work in [11] allows one to exploit the full degrees of freedom offered by the frequency selective wiretap channel to increase the security performance.

Information theoretic limits on secure communications over multi-path fading channels are investigated in [12] with OFDM. Secrecy capacity reduction due to an unconstrained eavesdropper is computed for the high signal to noise ratio (SNR) regime. Furthermore, the impact of different channel conditions between the legitimate parties and the eavesdropper on the secrecy capacity is evaluated.

More recently, a solution to secure communications over frequency selective fading channels has been proposed in [13]. The achieved secrecy is quantified using the concept of secrecy outage probability. Deep faded sub-channels are considered as the "null space" of the frequency selective single-input single-output (SISO) channel and they are filled by noise and are not used for transformation of useful information.

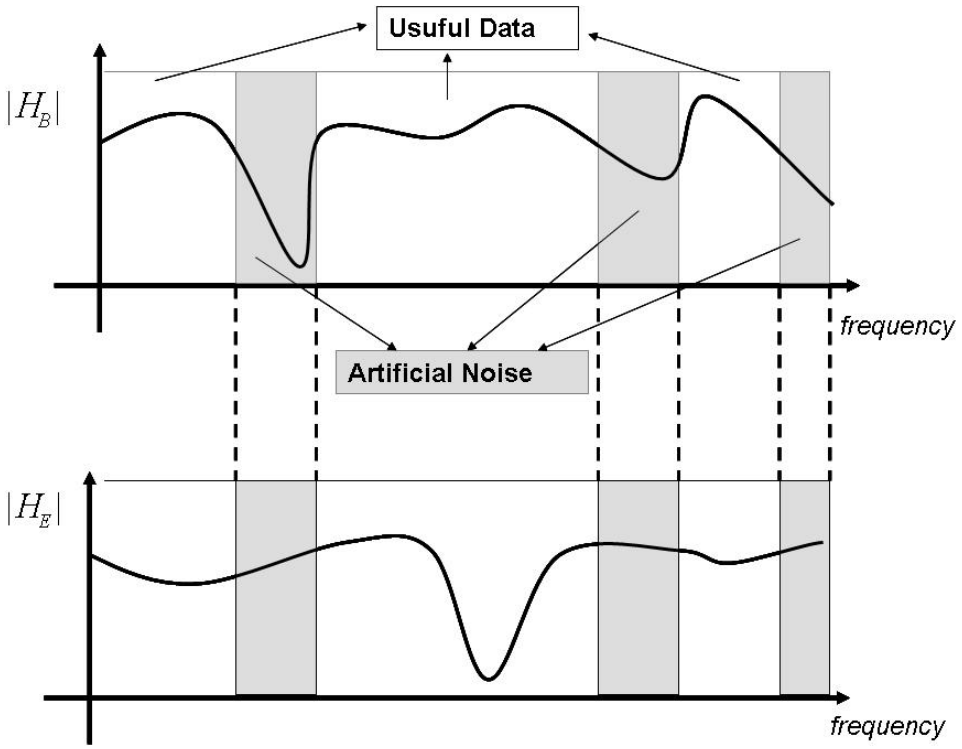

Figure 2.4: Intelligent sub-channel usage between transmitter and legitimate receiver deteriorating the signal quality captured by eavesdropper.

The idea behind the scheme proposed in [13] is illustrated in Figure 2.4. Transmitter employs only the sub-channels on which she experiences relatively good channel gains for the transmission of useful information towards the legitimate receiver, and avoids transmission over the deep faded subchannels. Hence the performance reduction over the main channel is minimized. However, Eve's receiving performance degrades due to the unused sub-channels on the transmit channel. Also, using artificial noise in the unused sub-channels, a further degradation is obtained in Eve's reception performance.

2.5 Chapter Summary

In this chapter, we presented a brief description of frequency selective fading channels and their features. We then discussed basics of OFDM scheme and its advantages over frequency selective fading channels. We also studied secrecy capacities and achievable rates for AWGN channels and fading channels with different assumptions on the transmitter's knowledge of the channel state information. Finally, we reviewed the current literature on the physical layer security over frequency selective fading channels.

Chapter 3

Secrecy Rates of Frequency Selective Fading Channel with Perfect CSIT

In this chapter, we consider transmission of secret messages over frequency selective fading channels assuming that OFDM is employed. We model this system as an instance of a high dimensional MIMO wiretap channel and derive the optimal power allocation for the scenarios where perfect CSI of the main channel and the eavesdropper's channel is available at the transmitter. Furthermore, we study the effects of user's mobility on the secrecy rates over frequency selective fading channels. In addition, for the scenarios where the transmitter has CSI of the main channel only, we derive an achievable rate with the assumption that the transmitter adopts a water-filling power allocation method as a sub-optimal policy. Finally, we compare the secrecy rates achieved by these two scenarios to quantify the loss in the achievable secrecy rates in the absence of the CSI corresponding to eavesdropper's channel.

This chapter is organized as follows. In Section 3.1, the optimal power allocation for frequency selective fading channels is described when the transmitter knows the CSI of both channels. A low complexity alternative for the maximization of the achievable secrecy rates is introduced in Section 3.2. Then, the effects

of mobility on the achievable secrecy rates are investigated in Section 3.3. In Section 3.4, with an assumption that the transmitter employs waterfilling power allocation based on the main channel CSI only, closed form expressions are derived for the capacity and the achievable rates over the main channel and the eavesdropper's channel. Finally, the numerical results are provided in Section 3.4.

3.1 Secrecy Rates with Full CSIT

In this section, we assume that at the beginning of each coherence interval, the transmitter has perfect channel state information of both the legitimate receiver and the eavesdropper. Both eavesdropper's and legitimate receiver's channels experience block fading. Channel gains remain constant during each coherence interval and change independently from one to another. The fading process is ergodic with a bounded continuous distribution. Furthermore, the fading coefficients of the eavesdropper and the legitimate receiver are assumed to be independent of each other in any coherence interval, and the coherence intervals are large enough to allow for invoking the random coding arguments [8].

Consider the system model whose block diagram is depicted in Figure 3.1. The signals received by the legitimate receiver and eavesdropper are given by

$$y_b(t) = \sum_{l=1}^{L_b} h_b(t,l)x(t-l) + w_b, \tag{3.1}$$

$$y_e(t) = \sum_{l=1}^{L_e} h_e(t,l)x(t-l) + w_e, \tag{3.2}$$

respectively, where h_b, h_e are the taps of the main channel and eavesdropper's channel, respectively. We assume that the multi-path fading channels consist of L_b and L_e resolvable paths whose gains are i.i.d. zero mean complex Gaussian random variables. w_b, w_e represent circularly symmetric complex i.i.d. additive Gaussian noise with zero mean and unit variance at the legitimate receiver and the eavesdropper, respectively.

Frequency response of the main channel, i.e., between the transmitter and the

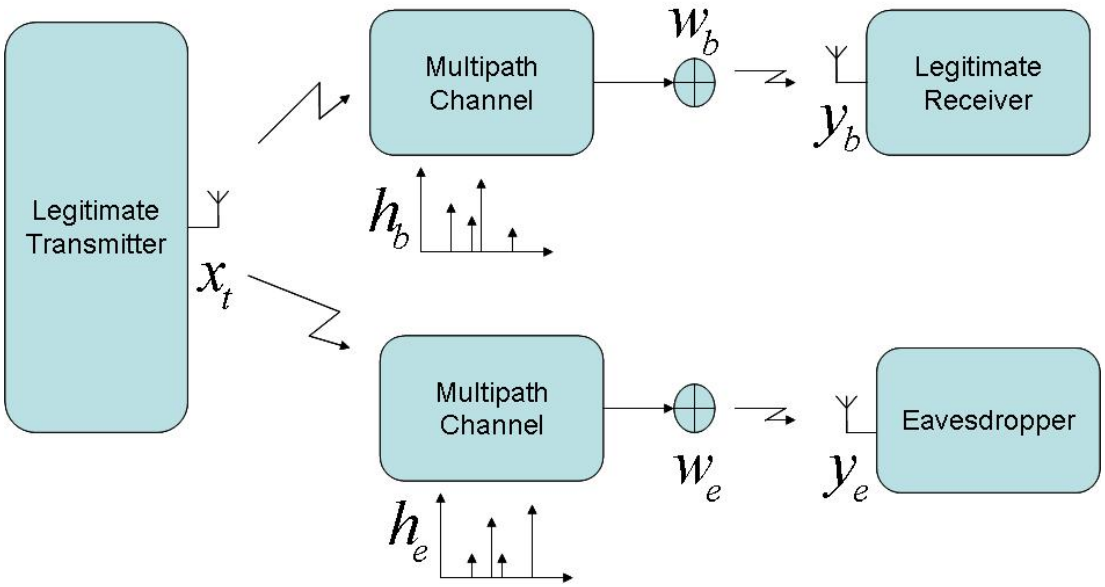

Figure 3.1: Block diagram of the system model.

legitimate receiver is found by discrete Fourier transform (DFT) of tapped delay line. We assume that there are N sub-bands (with flat fading) approximating the frequency response of the channel. Signal received by the legitimate receiver can be written as

$$\begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{bmatrix} = \begin{bmatrix} H_0 & 0 & 0 & \dots & 0 \\ 0 & H_1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & H_{N-1} \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{bmatrix} + \begin{bmatrix} w_0 \\ w_1 \\ \vdots \\ w_{N-1} \end{bmatrix}, \tag{3.3}$$

where $x_0, \dots, x_{N-1}$ represent the transmitted signals on each sub-band. $w_0, \dots, w_{N-1}$ represent the noise terms. The diagonal elements of channel matrix are sub-channel gain of frequency selective fading channel. The diagonal elements of H matrix are the gain of the sub-channels.

Basically, we approximate the frequency selective fading channel via set of parallel Gaussian channels. A basic problem is the allocation of total available power across the sub-channels. This is similar to the power allocation problem for the independent parallel Gaussian channels. Each parallel independent channel can be considered as a sub-channel of our frequency selective fading channel model.

Let us define H_{Ei}, H_{Bi} as the frequency responses of the eavesdropper and

legitimate receiver channels at the i^{th} sub-band, respectively. When H_{Ei} and H_{Bi} are known at the transmitter, one can easily say that if $|H_{Ei}|^2 > |H_{Bi}|^2$ no power should be allocated for this band. For the cases where $|H_{Bi}|^2 > |H_{Ei}|^2$, assuming that a power of P_i is allocated to the band, the secrecy capacity of the sub-channel is

$$f(P_i) = log_2\left(1 + \frac{|H_{Bi}|^2 P_i}{\phi_{Bi}}\right) - log_2\left(1 + \frac{|H_{Ei}|^2 P_i}{\phi_{Ei}}\right), \tag{3.4}$$

where ϕ_{Ei} and ϕ_{Bi} are the noise powers for the eavesdropper and the legitimate receiver, respectively. Achievable secrecy rate is the sum of secrecy capacities of the sub-channels. The question is that how the transmitter should allocate its power to maximize the secrecy capacity. The optimal power allocation method that achieves the secrecy capacity in the case where both channels are known can be found by using a Lagrangian maximization approach as outlined below.

The secrecy rate maximization problem for a given power constraint can be written as

$$\max_{P(i)} \sum_{i=1}^{N} \left[log_2\left(1 + P_i \frac{|H_{Bi}|^2}{\phi_{Bi}}\right) - log_2\left(1 + P_i \frac{|H_{Ei}|^2}{\phi_{Ei}}\right)\right]^+ \tag{3.5}$$

such that

$$E\left[\sum_{i=1}^{N} P_i\right] \leq P_c, \tag{3.6}$$

where P_i is a function of H_{Bi} and H_{Ei}. P_c represents total power that will be allocated to all the sub-carriers. The Equation (3.5) is concave if $H_{Ei} \leq H_{Bi}$ [8] because it is well-known that nonnegative weighted sums (or integrals) preserve convacity [16]. As a result, the objective function is concave in P_i. The Lagrangian can be written as

$$L(P_i, \lambda) = \frac{1}{ln2} \sum_{i=1}^{N} \left[ln\left(1 + P_i \frac{|H_{Bi}|^2}{\phi_{Bi}}\right) - ln\left(1 + P_i \frac{|H_{Ei}|^2}{\phi_{Ei}}\right)\right] - \lambda\left(\sum_{i=1}^{N} P_i - P_c\right). \tag{3.7}$$

Then

$$\frac{\partial L(P_i, \lambda)}{\partial P_i} = \frac{1}{ln2}\left(\frac{|H_{Bi}|^2}{\phi_{Bi} + P_i|H_{Bi}|^2} - \frac{|H_{Ei}|^2}{\phi_{Ei} + P_i|H_{Ei}|^2}\right) - \lambda = 0, \tag{3.8}$$

$$\frac{\partial L(P_i,\lambda)}{\partial \lambda} = \sum_{i=1}^{N} P_i - P_c = 0. \tag{3.9}$$

The solution for this optimization problem can be obtained as

$$P_i = \frac{1}{2}\left[\sqrt{\left(\frac{\phi_{Ei}}{|H_{Ei}|^2} - \frac{\phi_{Bi}}{|H_{Bi}|^2}\right)^2 + \frac{4}{\lambda}\left(\frac{\phi_{Ei}}{|H_{Ei}|^2} - \frac{\phi_{Bi}}{|H_{Bi}|^2}\right)} - \left(\frac{\phi_{Bi}}{|H_{Bi}|^2} + \frac{\phi_{Ei}}{|H_{Ei}|^2}\right)\right]. \tag{3.10}$$

For some channel realization for Equation (3.10) power can be negative. In that case optimal value of power is zero. Thus the solution should be rewritten as

$$P_i = \frac{1}{2}\left[\sqrt{\left(\frac{\phi_{Ei}}{|H_{Ei}|^2} - \frac{\phi_{Bi}}{|H_{Bi}|^2}\right)^2 + \frac{4}{\lambda}\left(\frac{\phi_{Ei}}{|H_{Ei}|^2} - \frac{\phi_{Bi}}{|H_{Bi}|^2}\right)} - \left(\frac{\phi_{Bi}}{|H_{Bi}|^2} + \frac{\phi_{Ei}}{|H_{Ei}|^2}\right)\right]^+, \tag{3.11}$$

where λ is selected in such a way that $\sum_{i=1}^{N} P_i = P_c$ is satisfied. We note that the solution to power allocation policy for frequency selective fading channels is similar to the case of independent parallel Gaussian channels [17].

3.2 A Low Complexity Power Allocation Algorithm

In this section, we propose a low complexity algorithm for the maximization of secrecy rates over frequency selective fading channels. We assume that the transmitter has full CSI. Both channel gains change independently from one coherence interval to the next and remain constant in any coherence interval. In the previous section, for every channel realization, the constant λ which is related to power constraint is calculated by sweeping the values for λ step by step in a specific interval which may be undesirable in practical systems, hence motivating this simple algorithm.

First, it should be noted that when the channel has a single tap, i.e., the frequency response is flat, the power allocation is performed in an on/off manner. That is to say, when $H_B > H_E$ the entire power is allocated and if $H_B < H_E$ no

power is assigned. We now consider a case where there are two flat sub-channels in the frequency domain. In this case, the power allocation can be performed easily by a simple calculation without any need for sweeping over λ. Let us give a simple example.

Consider the two simple channels given in Figure 3.2. Let us find the power allocation that maximize the secrecy capacity, when total power is required to be less than 10. In other words, we want to find x shown in Figure 3.3.

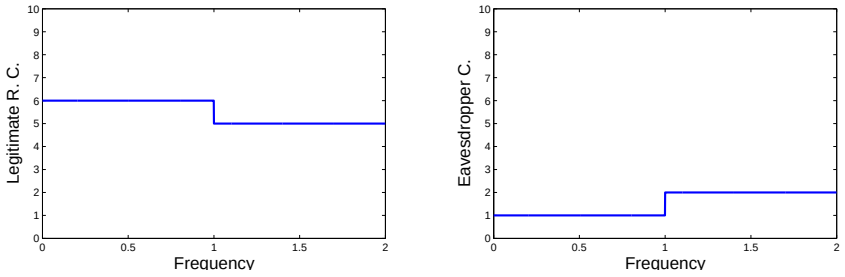

Figure 3.2: Example of legitimate and Eavesdropper channels.

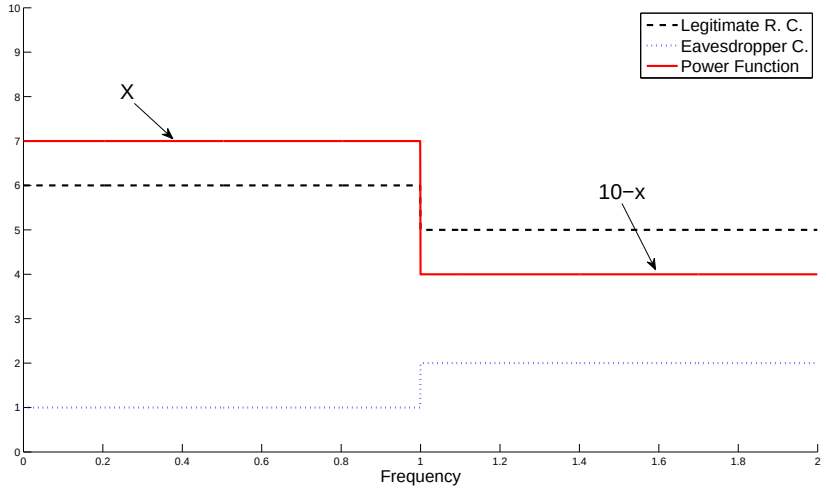

Figure 3.3: Power allocation on legitimate and Eavesdropper channels.

Consider the secrecy rate expression

$$C = ln(1 + 5x) + ln(1 + 6(10 - x)) - ln(1 + x) - ln(1 + 2(10 - x)), \quad (3.12)$$

and taking the derivative with respect to the unknown x we obtain

$$\frac{\partial C}{\partial x} = \frac{5}{1+5x} - \frac{6}{1+6(10-x)} - \frac{1}{1+1x} + \frac{2}{1+2(10-x)} = 0, \tag{3.13}$$

hence the optimal value of x is 6.047.

Clearly, when there are only two flat sub-channels in the frequency domain, the power allocation is simple. For the general case with N sub-channels, as an extension we propose the following algorithm. Firstly, discard the sub-channels with $H_{Bi} < H_{Ei}$, i.e., allocate no power. Then,

1- Divide the entire frequency band in half.

2- Sum magnitudes of the channel gains of sub-channels for each part.

3- Allocate power for both parts following simple example above.

4- Proceed for $\lfloor log_2(N) \rfloor$ iterations.

Let us give a numerical example that studies the performance of the proposed algorithm. Simulation results depicting the achieved secrecy rates for optimum and the proposed low complexity algorithm are given in Figure 3.4. Frequency response of the channel is found as follows. First, we generate complex valued taps in time domain, whose components are circularly symmetric complex Gaussian random variables with zero mean 1/2 variance per dimension, for both legitimate receiver and eavesdropper. Number of taps are fixed to 12. Tap delays are uniformly chosen in interval between 0 ns and 5000ns, and the corresponding frequency responses of the channels are found by using DFT.

It can be seen from the Figure 3.4 that the gap between the optimal solution and the proposed low complexity one is around 3-4dB.

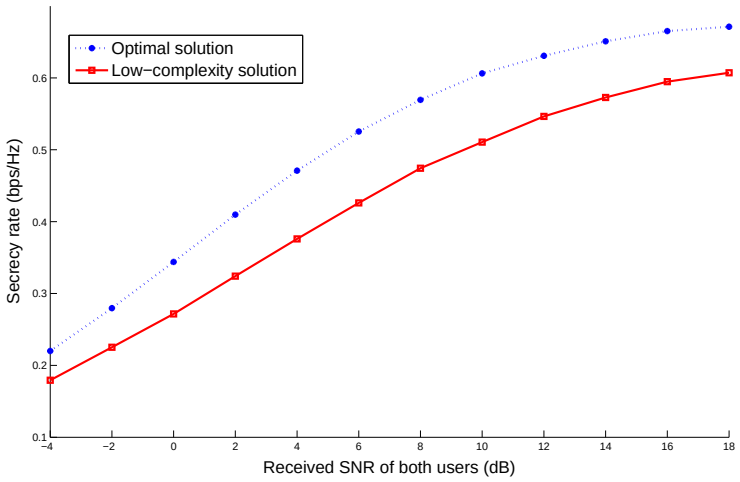

Figure 3.4: Comparison of optimal and low complexity solutions for power allocation.

3.3 OFDM Transmission over Time-Varying Multipath Channels

Consider a scenario in which the legitimate receiver and/or the eavesdropper has motion, and the transmitter has the knowledge of main channel and eavesdropper's channel at the beginning of each coherence interval. In the previous section, we showed that when there is no motion, frequency selective fading channels can be considered as parallel independent Gaussian channels. When the channel is time varying, the resulting model (with the use of OFDM) is no longer parallel Gaussian as there will be ICI.

In this section, assuming that the transmitter uses the optimal power allocation method which is formulated in the previous section, we utilize the OFDM scheme to understand effects of mobility on the security metrics. Power allocation is done by using the knowledge of the channel realization at the beginning of each transmission interval. In the presence of ICI, the channel matrices (for the

OFDM transmission) are no longer diagonal. They are, however, banded matrices where the off-diagonal elements have increased powers in the case of higher mobility.

3.3.1 System Model

Samples of an OFDM word are obtained by the inverse fast Fourier transform

$$x_n = \sum_{m=0}^{N-1} X_m e^{j2\pi nm/N}, \quad 0 \leq n \leq N-1, \tag{3.14}$$

where x_n is the n^{th} sample of OFDM word, X_m is input data for m^{th} sub-carrier, and N is the number of sub-carriers. Assuming a fading channel with L resolvable paths, the received signal can be expressed as

$$z_n = \sum_{l=0}^{L-1} h_{n,l} x_{n-l} + w_n, \tag{3.15}$$

where w_n represents the AWGN sample at time n, and $h_{n,l}$ is the complex valued channel gain for the l^{th} path at time n. For simplicity, we do not take into account the cyclic prefix that is used to prevent inter-symbol interference (ISI) and simply assume that it is removed at the receiver. The demodulated signal is then obtained by taking fast Fourier transform of z_n

$$Y_m = \sum_{i=0}^{N-1} \sum_{l=0}^{L-1} X_i H_l^{m-i} e^{-j2\pi li/N} + W_m, \tag{3.16}$$

where W_m is FFT of the noise vector (which is again white Gaussian). We can write

$$Y_m = \left\{ \sum_{l=0}^{L-1} H_l^0 e^{-j2\pi lm/N} \right\} X_m + \sum_{i=0, i\neq m}^{N-1} \sum_{l=0}^{L-1} X_i H_l^{m-i} e^{-j2\pi li/N} + W_m, \tag{3.17}$$

where H_l^{m-i} is the FFT of $h_{n,l}$

$$H_l^{m-i} = \frac{1}{N} \sum_{n=0}^{N-1} h_{n,l} e^{-j2\pi n(m-i)/N}. \tag{3.18}$$

When there is no mobility, H_l^{m-i} terms are zero and, the second term of the Equation (3.17) vanishes. In the general case, however, we have

$$\begin{bmatrix} Y_0 \\ Y_1 \\ \vdots \\ Y_{N-1} \end{bmatrix} = \begin{bmatrix} \alpha_{0,0} & \alpha_{1,0} & \dots & \alpha_{0,N-1} \\ \alpha_{1,0} & \alpha_{1,1} & \dots & \alpha_{1,N-1} \\ \vdots & & \ddots & \vdots \\ \alpha_{N-1,0} & \alpha_{N-1,1} & & \alpha_{N-1,N-1} \end{bmatrix} \begin{bmatrix} X_0 \\ X_1 \\ \vdots \\ X_{N-1} \end{bmatrix} + \begin{bmatrix} W_0 \\ W_1 \\ \vdots \\ W_{N-1} \end{bmatrix}, \tag{3.19}$$

where the $\alpha_{i,j}$ is given by

$$\alpha_{i,k} = \sum_{l=0}^{L-1} H_l^{i-k} e^{-j2\pi kl/N}. \tag{3.20}$$

Note that this models both the main user's and eavesdropper's channels (with different path gains and delays). When there is the mobility, there is ICI and we can treat the channel as the MIMO channel in which the sub-carriers are thought as different antennas, the number of sub-carriers can be considered as the number of transmit and receive antennas. In other words, the secrecy problem turns into the that of MIMO channel.

3.3.2 Solution Approach

The power allocation issue for frequency selective fading channels can be considered as power allocation problem for multiple-input multiple-output multiple-antenna-eavesdropper (MIMOME) systems. Secrecy capacity for MIMOME wiretap channel has been derived in [18]. Here, we model the OFDM transmission over a single-input single-output (SISO) wiretap channel as a MIMOME wiretap channel with $N \times N$ (not necessarily diagonal) channel matrices, where N is the number of subcarriers. We assume that the CSI of the legitimate receiver and the eavesdropper are known at transmitter at the beginning of the each transmission block. Then, conditioned on the channel gains, the secrecy capacity can be written as [18];

$$C = \max_{K_P \in K_S} log \frac{det\left(I + H_b K_P H_b^\dagger\right)}{det\left(I + H_e K_P H_e^\dagger\right)}, \tag{3.21}$$

where H_b and H_e are the channel matrices of legitimate receiver and eavesdropper, respectively. $(.)^\dagger$ refers to Hermitian operation. I is the $N \times N$ identity matrix, and K_P donates covariance matrix of input ($x \sim \mathcal{CN}(0, K_P)$), where $\mathcal{CN}$ donates circularly symmetric complex Gaussian random vector with zero mean and covariance K_P. K_S is defined as

$$K_S = \{K_P : K_P \succeq 0, tr(K_P) \leq P_c\}. \tag{3.22}$$

Finding the input covariance matrix that satisfies Equation (3.21) is a non-convex optimization problem whose solution satisfies the Karush-Kuhn-Tucker (KKT) conditions associated with Equation (3.22) [8].

The effects of mobility of users are investigated by using the power allocation method given in Section 3.1 by only utilizing the diagonal channel gains obtained with the channel coefficients at the beginning of the transmission. In other words, the only difference between no mobility and mobility cases is that, the transmitter performs power allocation based on the outdated channel state information and disregards the ICI terms. The fading process is ergodic, so we generate a large number of the channel realizations, and take the average of resulting rates to obtain achievable secrecy rates, i.e.,

$$R = E_{H_b,He}\left[[I(x, y|H_b) - I(x, z|H_e)]^+\right], \tag{3.23}$$

where $I(x, y|H_b)$ refers to mutual information between the channel input and the signal received at the legitimate receiver, given H_b. Similarly $I(x, z|H_e)$ stands for the mutual information between the transmitted signal and the eavesdropper's observation, given H_e [8].

3.3.3 Numerical Examples

In this subsection, we investigate the effects of mobility on the achievable secrecy rates via several numerical examples. Firstly, we need to design a set of uncorrelated channel realizations for each tap of the multipath channels modelling the legitimate user's and the eavesdropper's channels. For this purpose, we utilize the method of exact Doppler spread (MEDS) which is described in [19]. After

modelling the behaviour of each path of the multi-path channel, corresponding frequency domain matrices of both channels can be found by using the Equation (3.20).

The MEDS generates multiple uncorrelated Rayleigh fading processes with the approach of deterministic sum of sinusoids (SOS). That is, K mutually uncorrelated fading waveforms are generated by using an SOS channel simulator

$$\mu_i^k(t) = \sqrt{\frac{2}{N_i}} \sum_{n=1}^{N_i} \cos(2\pi f_{i,n}^k t + \theta_{i,n}^k), i = 1, 2, k = 1, 2, \ldots, K, \tag{3.24}$$

where $f_{i,n}^k$ is discrete Doppler frequency. $\theta_{i,n}^k$ represent phases of n^{th} sinusoid of the real component $\mu_1^k(t)$ and imaginary component $\mu_2^k(t)$ of the k^{th} complex waveform. The phases $\theta_{i,n}^k$ are i.i.d. uniform random variables over the interval $[0, 2\pi]$. N_i represents number of sinusoids used. This process is depicted in Figure 3.5.

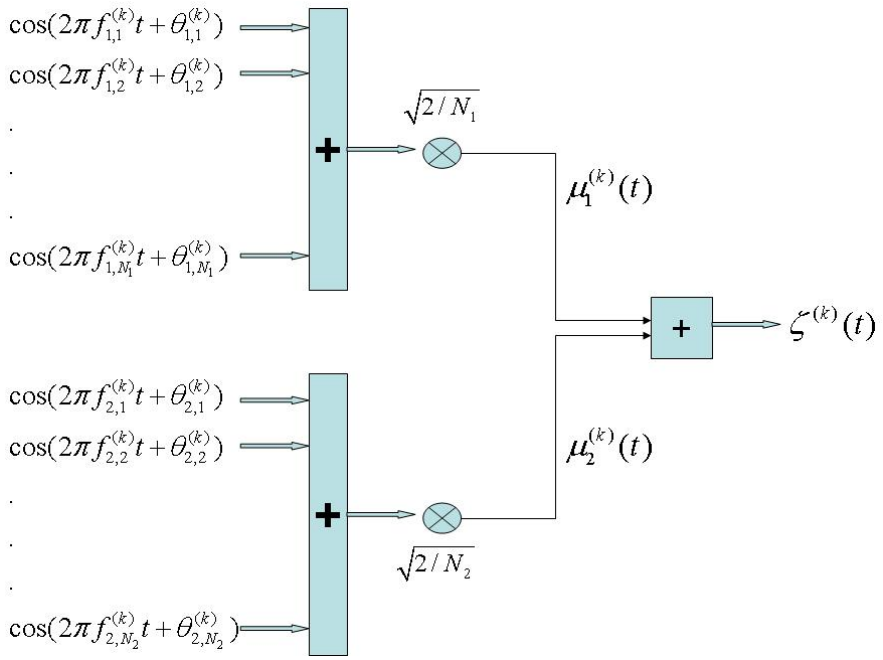

Figure 3.5: Structure of the SOS channel simulator for Rayleigh fading channels.

We provide a few examples of the channel matrices that are found by using the MEDS, as represented in Figures 3.6 and 3.7. The parameters are as follows; 32 sub-carriers are used and sampling frequency is 256 kHz, and 4 channel taps are

considered where the maximum tap delay is $5\mu s$ and the carrier frequency is 4.4 GHz.

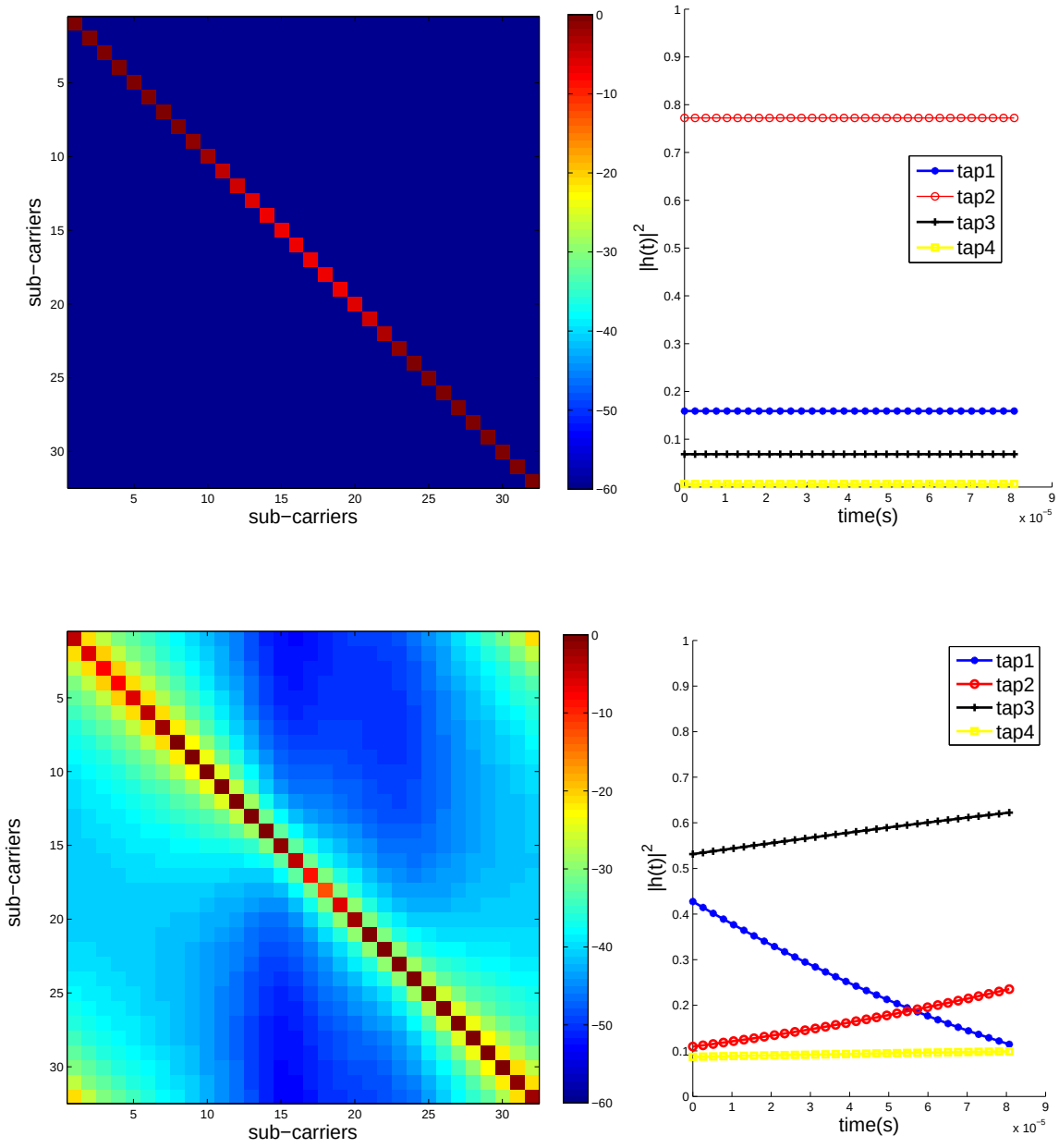

Figure 3.6: Simulation of the time domain channels and frequency domain channel matrices when the velocities are 0km/h, 100km/h, respectively.

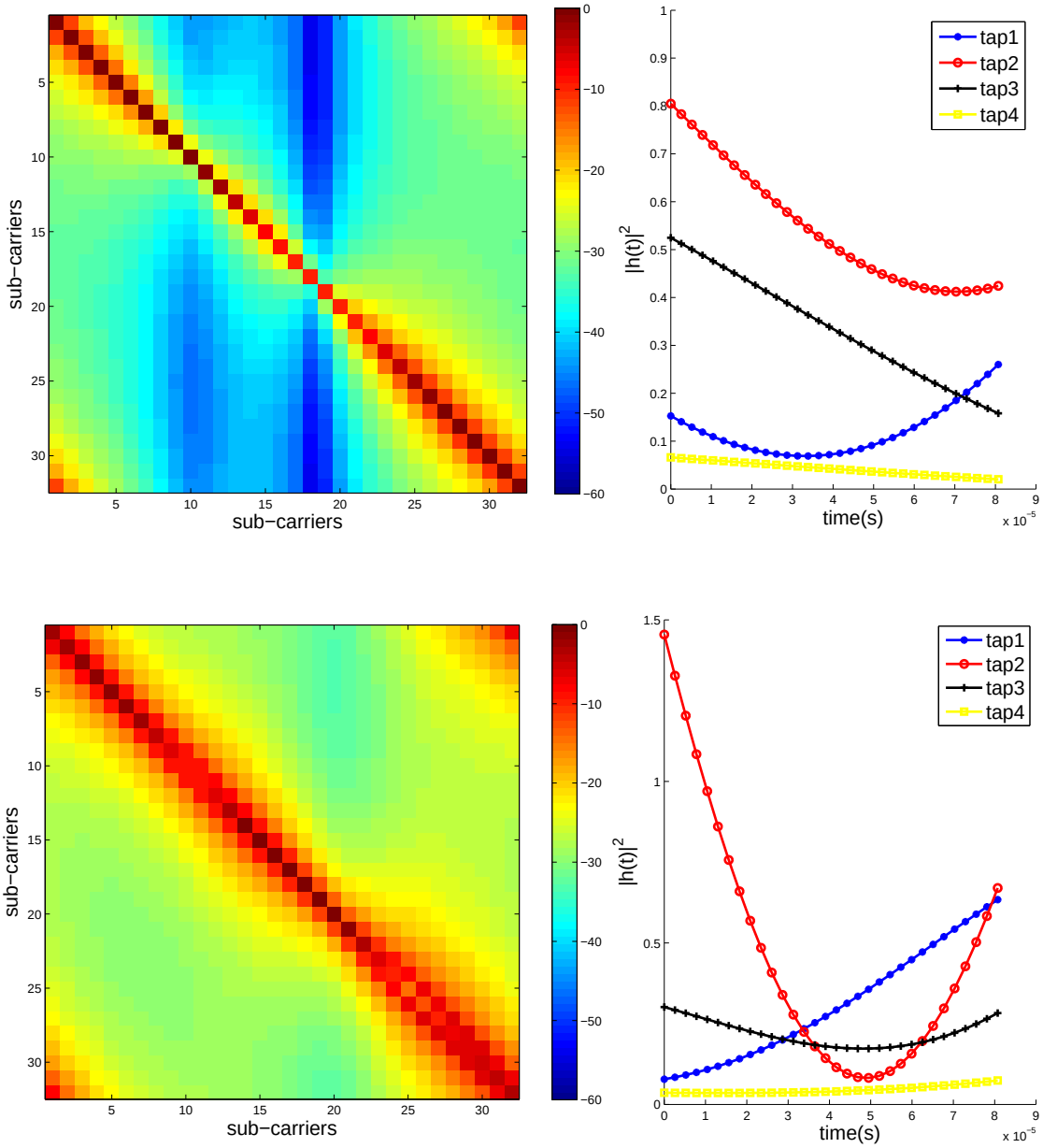

Figure 3.7: Simulation of the time domain channels and frequency domain channel matrices when the velocities are 300km/h, 600km/h, respectively.

It is clear that when there is motion, the corresponding channel matrix is no longer diagonal. As the rapidity of the time variations is increased, the effects of sub-carriers on their neighbours are also increased causing larger inter-carrier interference.

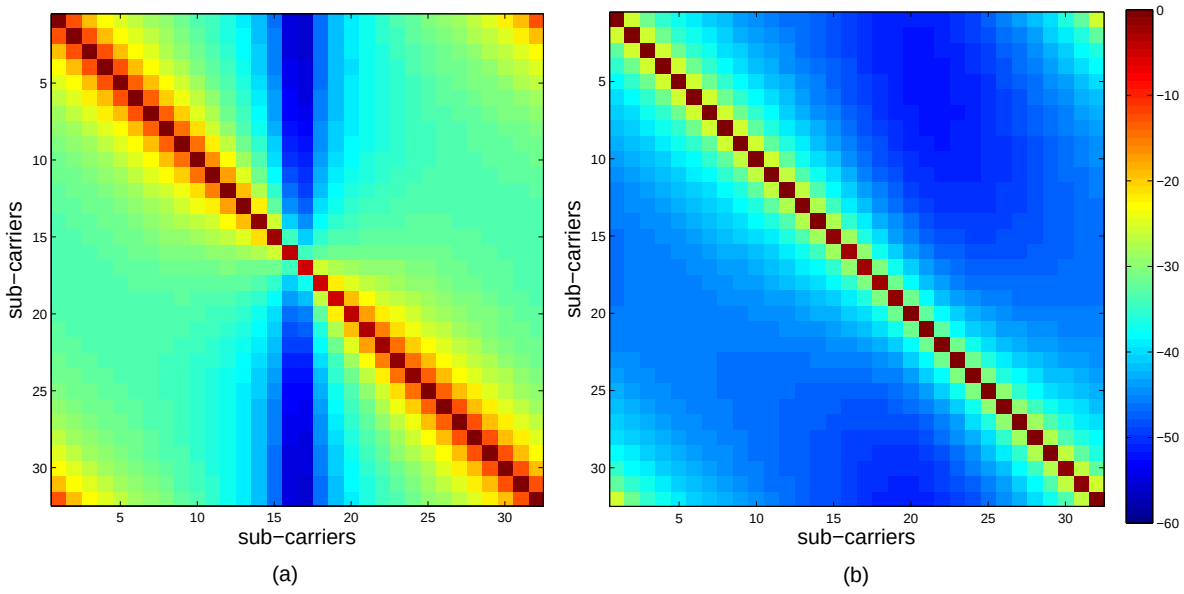

Figure 3.8: (a) Channel matrix for the signal bandwidth is 256 kHz (b) Channel matrix for the signal bandwidth is 340 kHz.

As a further example, we also provide the corresponding channel matrices for two different bandwidths used in Figure 3.8. The velocity of the user is fixed as 100 km/h in this example. Number of sub-carriers is also fixed to 32. Since the sub-carrier spacing is linearly proportional to signal bandwidth, and with increased sub-carrier spacing, the OFDM transmission will be more robust to ICI. This is clearly observed in Figure 3.8.

We perform the power allocation at the transmitter by using the knowledge of both channel matrices at the beginning of each OFDM word transmission. Since the channel is time-varying due to mobility, the channel matrix estimates at the transmitter are outdated during the transmission. We expect that due to using

the outdated channel matrices, there will be losses in the achievable secrecy rates compared to the case with exact channel knowledge.

We now present several numerical examples to study the effects of mobility on secrecy rates via Monte Carlo simulations. We assume that the real and imaginary components of the channel taps are i.i.d. circularly symmetric Gaussian random variables with zero mean and variance 1/2 per dimension. Delays of the channel taps are chosen between 0 to 5000ns uniformly. The MEDS is used with the number of sinusoids selected as 30 to generate realizations of the channel coefficients. The sub-carrier spacing is 8 kHz, and the number of sub-carriers is 32. Carrier frequency is 4.4 GHz, and sampling frequency is 256 kHz.

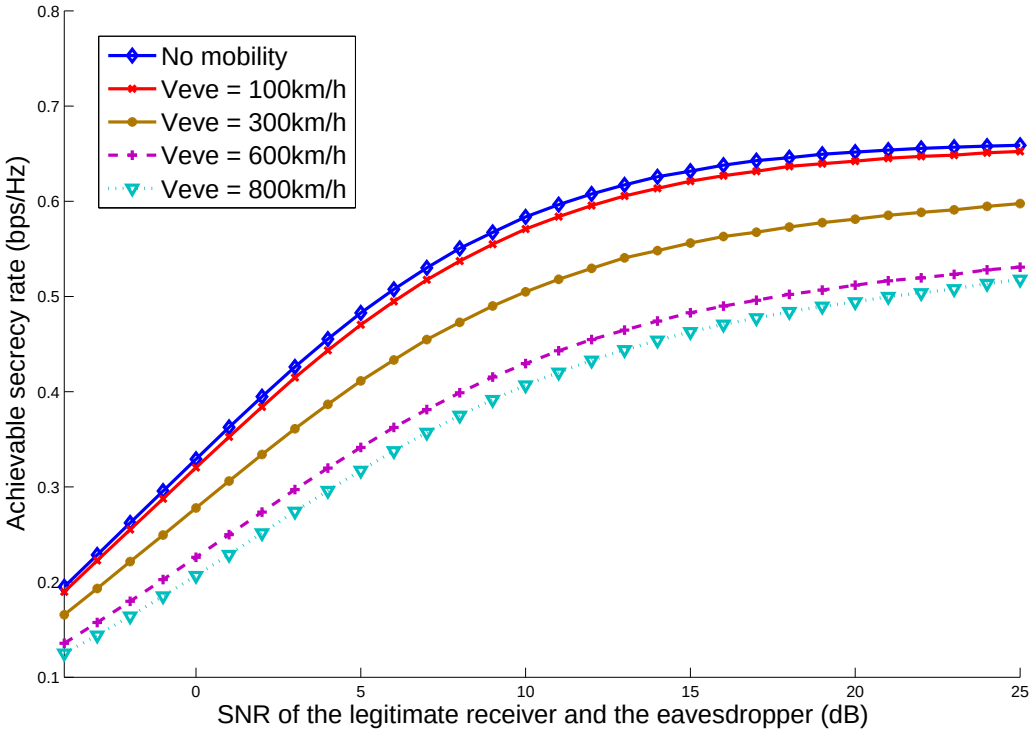

Figure 3.9: Secrecy rates, when the eavesdropper has mobility with different velocities, whereas the legitimate receiver is static.

First, we consider the effects of eavesdropper's mobility on the achievable secrecy rates. The legitimate receiver is static over the OFDM word, i.e., the channel of legitimate receiver experiences block fading. The power allocation at the transmitter is performed by using the optimum power allocation strategy with the perfect knowledge of channel of legitimate receiver and the knowledge of eavesdropper's channel at the beginning of each transmission block.

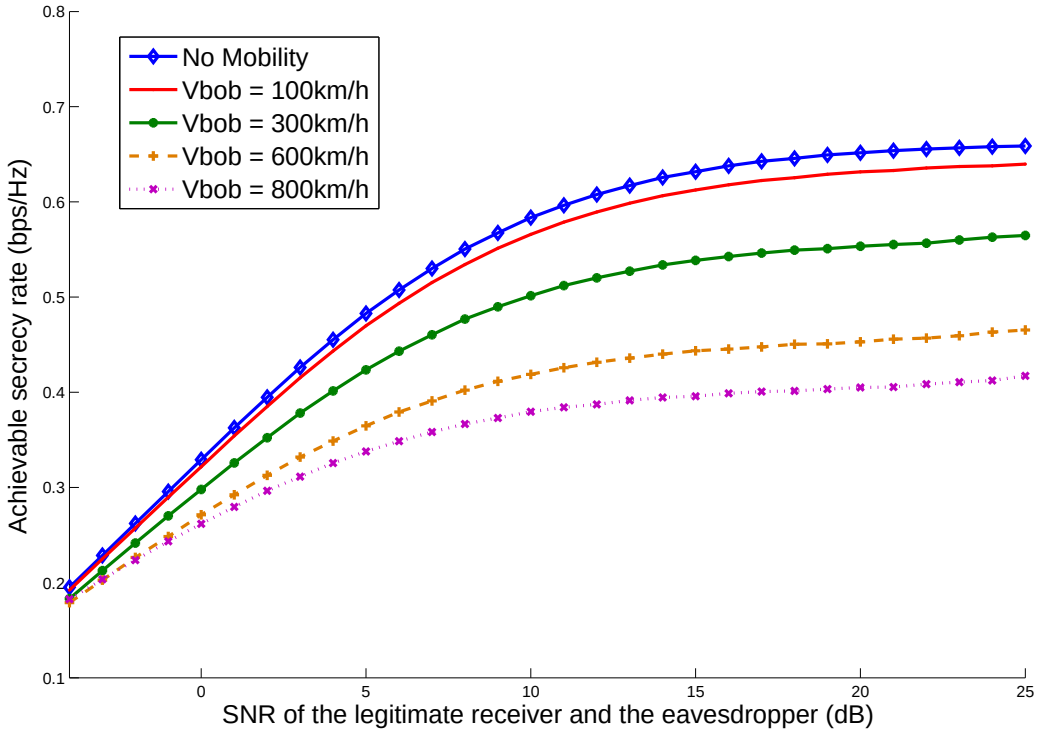

Figure 3.10: Secrecy rates, when the legitimate receiver has mobility with different velocities, whereas the eavesdropper is static.

The effects of eavesdropper's mobility on secrecy rates are depicted in Figure 3.9. If the speed of eavesdropper is increased with respect to the transmitter, the taps of eavesdropper's channel vary faster. This increases the difference between the actual channel and the channel knowledge which is employed for the power allocation. We observe that, when the speed of eavesdropper is under 100km/h,

secrecy rate is changed only slightly. However, the significant effects can be seen when the speed is over 100km/h.

Consider a new scenario in which the eavesdropper is static with respect to the transmitter whereas the legitimate receiver has mobility. The parameters are the same as the previous simulation except for velocity of the legitimate receiver and eavesdroppers. The results are as shown in 3.10.

We observe that when the mobility of the legitimate receiver is increased, the secrecy rate is decreased due to the power leakage to neighbouring sub-carriers of the legitimate receiver. In this case, the effects of mobility is more severe at the velocities over 100km/h compared to the previous examples.

3.4 Security with Only Main Channel CSI at the Transmitter

In this section, we assume that at the beginning of each coherence interval, the CSI of the main channel and only a statistical knowledge of the eavesdropper's channel are available at transmitter. The channel experiences block fading, i.e., the fading coefficients change from one coherence interval to the next independently and are constant within each coherence interval. Both channel gains are ergodic with a bounded continuous distribution.

As a sub-optimal solution a water-filling based power allocation algorithm is utilized at transmitter using only the main channel knowledge. The idea is to use the optimum power allocation policy for maximization of the mutual information over the main channel [20], however, for the secrecy capacity problem this is not necessarily the best. We derive a closed form expression for both user's capacities, and compare the secrecy performances of different power allocations.

3.4.1 Water-Filling Power Allocation

Consider a channel which is discrete-time, band-limited with additive Gaussian noise, subdivided into N sub-carriers. Assume that the channel response is approximately constant in a bandwidth Δf which is the sub-carrier spacing. If we denote the signal power, channel frequency response and additive Gaussian noise power of the sub-channel by P_k, H_k and ϕ_k, respectively, the channel capacity can be expressed as [21];

$$C = \sum_{k=1}^{N} log_2[1 + (P_k|H_k|^2/\phi_k)]. \tag{3.25}$$

The power allocated to each sub-carrier P_k is the same for uniform power allocation. On the other hand, in a frequency selective fading channel, at each time instance, some sub-carriers experience deep fading while others may experience relatively good channel gains. When there is no unintended receiver the optimal power allocation method is water-filling [22], that is, when the transmitter has a perfect knowledge of the channel of the legitimate receiver, capacity over the main channel can be written as

$$C_{Bob} = \sum_{i=1}^{N} log_2 \left[1 + max\left(K - \frac{\Phi_{Bi}}{|H_{Bi}|^2}, 0\right)\frac{|H_{Bi}|^2}{\Phi_{Bi}}\right]. \tag{3.26}$$

We assume that the eavesdropper also adopts an OFDM demodulator with cyclic prefix removal and FFT similar to the legitimate receiver [23]. The overall power allocation is performed based on the channel of the legitimate receiver at the transmitter, hence the channel capacity for the eavesdropper is

$$C_{Eve} = \sum_{i=1}^{N} log_2 \left[1 + max\left(K - \frac{\Phi_{Bi}}{|H_{Bi}|^2}, 0\right)\frac{|H_{Ei}|^2}{\Phi_{Ei}}\right]. \tag{3.27}$$

The achievable secrecy rate (conditioned on the channel gains) with this scheme is the difference between Bob's channel capacity and Eve's channel capacity, so

$$R_{Sec} = [C_{Bob} - C_{Eve}]^+. \tag{3.28}$$

To evaluate each term, we first find the distribution of $|H_k|^2$ to find the expected value of the capacity per sub-carrier. Denoting the real part of H_k by X_k and the

imaginary part by Y_k and assuming that X_k and Y_k are independent zero mean and variance $\sigma_k^2/2$ Gaussian random variables, i.e.,

$$H_k = X_k + jY_k, \tag{3.29}$$

the correlation between the coefficient X_{k_1} and X_{k_2} is computed as [24];

$$E[X_{k_1}X_{k_2}] = \frac{1}{2}\sum_{k=0}^{L-1}\sigma_k^2 cos\left[\frac{2\pi(k_1-k_2)\tau_k}{N}\right]. \tag{3.30}$$

Similarly,

$$E[Y_{k_1}Y_{k_2}] = \frac{1}{2}\sum_{k=0}^{L-1}\sigma_k^2 cos\left[\frac{2\pi(k_1-k_2)\tau_k}{N}\right], \tag{3.31}$$

$$E[X_{k_1}Y_{k_2}] = \frac{1}{2}\sum_{k=0}^{L-1}\sigma_k^2 sin\left[\frac{2\pi(k_1-k_2)\tau_k}{N}\right], \tag{3.32}$$

and

$$E[X_{k_1}Y_{k_2}] = -E[X_{k_2}Y_{k_1}], \tag{3.33}$$

where τ_k is the delay of the k^{th} path. L is the total number of resolvable paths and N denotes the number of sub-carriers. Note that, $|H_k|^2$ is sum of X_k^2 and Y_k^2, which is an exponential random variable with parameter $\frac{1}{\sqrt{2}\sigma_k^2}$.

3.4.2 Individual Rates in Closed Form

To find a closed form expression of the capacity of the legitimate receiver (with no secrecy constraint), we evaluate

$$\mu_C = E\left[\frac{1}{N}\sum_{k=1}^{N} C_b(k)\right]. \tag{3.34}$$

The capacity of k^{th} sub-carrier within an OFDM symbol is found in Equation (3.26);

$$E[C_b(k)] = \int_0^\infty log_2\left(1+\max\left(K-\frac{\phi_k}{y}\right)\frac{y}{\phi_k}\right)\frac{1}{\sqrt{2}\sigma_k^2}e^{-y/\sqrt{2}\sigma_k^2}dy, \tag{3.35}$$

where $y = |H_{Bk}|^2$,

$$E[C_b(k)] = \frac{1}{\sqrt{2}\sigma_k^2} \int_{\frac{\phi_k}{K}}^{\infty} log_2\left(\frac{Ky}{\phi_k}\right) e^{-y/\sqrt{2}\sigma_k^2} dy \tag{3.36}$$

then using $\frac{Ky}{\phi_k} = X$ and accordingly, $\frac{Kdy}{\phi_k} = dX$, we obtain

$$E[C_b(k)] = \frac{1}{\sqrt{2}\sigma_k^2} \frac{\phi_k}{K} \int_1^{\infty} log_2(X) e^{\frac{\phi_k X}{\sqrt{2}K\sigma_k^2}} dX. \tag{3.37}$$

We then get $\int_1^{\infty} e^{-x\mu} lnx dx = \frac{-1}{\mu} Ei(-\mu)$, where Ei is exponential integral function [25], given as

$$Ei(z) = -\int_{-z}^{\infty} \frac{e^{-t}}{t} dt. \tag{3.38}$$

The Equation (3.37) can be written as

$$E[C_b(k)] = \frac{1}{\sqrt{2}\sigma_k^2} \frac{\phi_k}{K} \frac{-\sqrt{2}K\sigma_k^2}{\phi_k} Ei\left(\frac{\phi_k}{-\sqrt{2}K\sigma_k^2}\right) \frac{1}{ln2}. \tag{3.39}$$

Finally, the closed form expression for the capacity of legitimate receiver (with no secrecy constraint) can be written as

$$E[C_b(k)] = -\frac{1}{ln2} Ei\left(\frac{\phi_k}{-\sqrt{2}K\sigma_k^2}\right). \tag{3.40}$$

The capacity of eavesdropper can be found similarly. Expected value of eavesdropper's capacity can be written as

$$E[C_e(k)] = \int_0^{\infty} \int_0^{\infty} log_2(1 + max(K - \frac{\phi_{Bk}}{y}, 0) \frac{x}{\phi_{Ek}}) \frac{1}{2\sigma_k^4} e^{-(x+y)/\sqrt{2}\sigma_k^2} dx dy \tag{3.41}$$

where $x = |H_{Ek}|^2$. To remove the max function, we change the limits of the integral

$$E[C_e(k)] = \frac{1}{ln(2)2\sigma_k^4} \int_{\frac{\phi_{Bk}}{K}}^{\infty} \int_0^{\infty} ln(1 + (K - \frac{\phi_{Bk}}{y}) \frac{x}{\phi_{Ek}}) e^{-y/\sqrt{2}\sigma_k^2} e^{-x/\sqrt{2}\sigma_k^2} dx dy. \tag{3.42}$$

Reorganizing, we obtain

$$E[C_e(k)] = \frac{1}{ln(2)2\sigma_k^4} \int_{\frac{\phi_{Bk}}{K}}^{\infty} e^{-y/\sqrt{2}\sigma_k^2} \int_0^{\infty} ln(1 + \beta x) e^{-\mu x} dx dy, \tag{3.43}$$

where β is $(K - \frac{\phi_{Bk}}{y})\frac{1}{\phi_{Ek}}$ and μ is $1/\sqrt{2}\sigma_k^2$ and from [25];

$$\int_0^\infty ln(1+\beta x)e^{-\mu x}dx = -1/\mu e^{\mu/\beta}Ei(-\mu/\beta). \tag{3.44}$$

Finally,

$$E[C_e(k)] = -\frac{1}{ln(2)2\sigma_k^4}\int_{\frac{\phi_{Bk}}{K}}^\infty e^{-y/\sqrt{2}\sigma_k^2}\frac{-1}{\mu}e^{\frac{\mu}{\beta}}Ei\left(-\frac{\mu}{\beta}\right)dx. \tag{3.45}$$

We found closed form expressions for the rates achieved by both the legitimate receiver and the eavesdropper above. The secrecy rate is the difference of Equations (3.40) and (3.45).

3.4.3 Numerical Results

In Figure 3.11, we compare the average capacity of the main channel which is attained by evaluation of the Equation (3.40) with the values of the average capacity obtained from Monte Carlo simulations. Clearly, analytical results match the simulation results as expected.

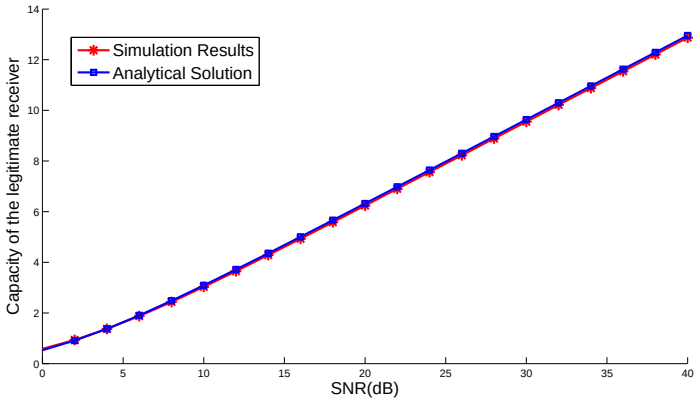

Figure 3.11: Analytical results of expected value of the legitimate receiver's channel capacity (with no secrecy constraint) and simulation results are compared.

We now provide a numerical example. We assume that the time domain channel state information of the legitimate receiver, i.e., the magnitude of the path gains and the related delays are known. Both users' channels are divided into 64 sub-channels. The time domain channel response of the frequency selective fading channel is obtained by the MEDS method in [19] as in the previous section. Then by using an FFT, the frequency responses are obtained. Path gains have zero mean unit variance i.i.d. complex Gaussian distributions. The channel has 12 fixed taps and relating delays are chosen uniformly in the interval between 0 and 5000ns.

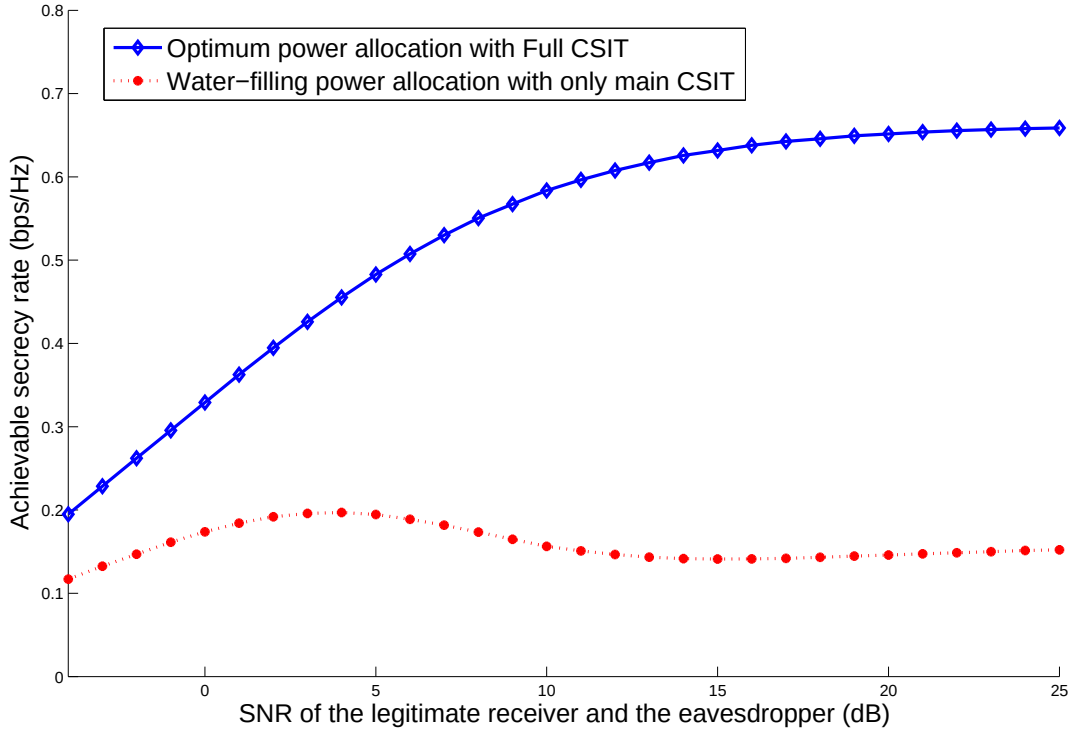

Figure 3.12: Achievable rate of water-filling algorithm with only knowledge of main CSIT, and the secrecy capacity with optimal power allocation with Full CSIT.

The performance of optimal power allocation with full CSIT and with the water-filling power allocation using only the main CSIT are depicted in Figure

3.12. While the SNRs of both the legitimate receiver and eavesdropper are increased, the rates achievable by the water-filling power allocation method fluctuates. This is explained by noting that the water-filling power allocation method is a sub-optimal solution and that both the SNR of the legitimate user and the eavesdropper are the same in this example. The best performance of water-filling method is for the SNRs ranging from 3dB to 4dB. Since the total power is allocated almost uniformly in the high SNR regime with the water-filling power allocation, the achievable rates saturate in high SNRs. Optimal power allocation performance also saturates at high SNRs.

3.5 Chapter Summary

In this chapter, we have studied secrecy rates over frequency selective fading channels. We started with the full CSI at transmitter assumption and described the optimal power allocation for maximization of the secrecy rates. Then, a low complexity algorithm was proposed as a sub-optimal solution. Furthermore, we studied the effects of users' mobility on the secrecy rates with sub-optimal power allocation based on outdated CSI. Finally, we studied the performance of water-filling power allocation algorithm over the frequency selective fading channels for the case where only main CSI is available at the transmitter. The results reveal that in the absence of the eavesdropper's CSI, the achievable secrecy rates undergo a considerable loss with respect to the perfect CSI case.

Chapter 4

Secrecy for Frequency Selective Fading Channels with Quantized CSIT

In this chapter, we study the impact of quantized channel state information at the transmitter on the achievable secrecy rates over frequency selective fading channels. When only a quantized version of main channel state information is available at transmitter, a water-filling power allocation is employed and the secrecy rate loss due to the limited feedback channel is quantified through numerical examples. Our results demonstrate that this limited information on the main channel can still be helpful in achieving positive secrecy rates.

4.1 System Model and Problem Description

A transmitter wants to send its messages to a legitimate receiver over a frequency selective fading channel. The legitimate receiver has a perfect knowledge of its channel. However, the transmitter acquires only a quantized CSI in the following manner. The legitimate receiver and the transmitter have in common

a randomly generated codebook for quantization. The legitimate receiver sends the index of a codeword in the codebook to describe the current realization of its channel. The transmitter obtains an estimate of the CSI by decoding this codeword, and then, it uses this quantized CSI to allocate power across different frequencies by using water-filling.

The system model is depicted in Figure 4.1. The main channel is estimated at the transmitter, then power is allocated dynamically using information of quantized delay taps. Single-carrier frequency-domain equalization (SC-FDE) [26] and OFDM based systems are well-known examples that enable dynamic spectrum usage with a simple DFT based implementation. In this chapter, we employ the OFDM scheme.

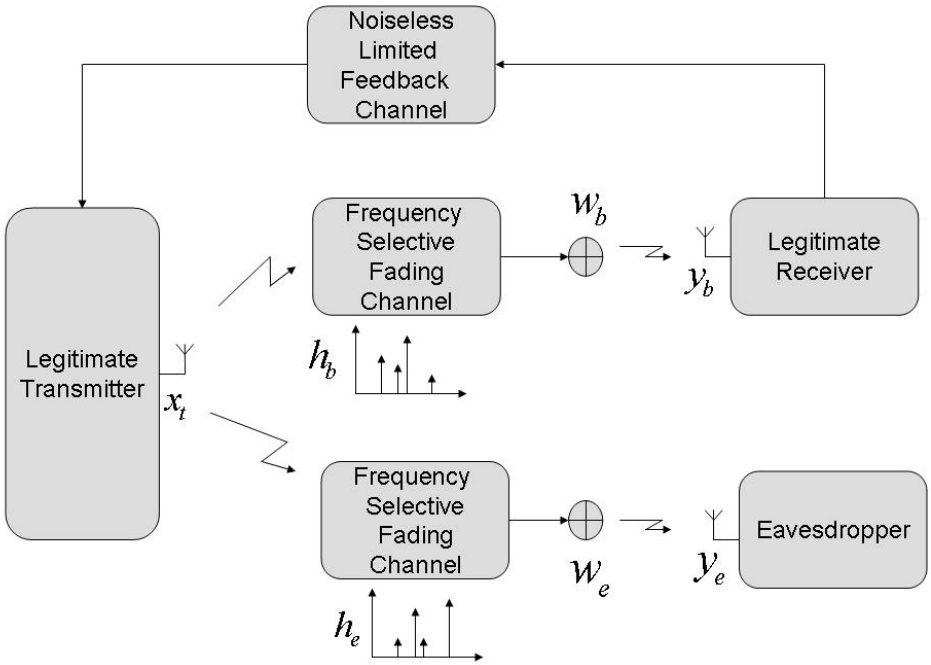

Figure 4.1: Block diagram of the system model.

We assume that both the legitimate receiver and the eavesdropper channels experience block fading where the channel gains remain constant during each coherence interval and change independently from one coherence interval to the next. The fading process is assumed to be ergodic with a bounded continuous

distribution. In addition, the fading coefficients of the legitimate receiver and the eavesdropper are assumed to be independent of each other in each coherence interval. Moreover, each coherence interval is large enough to allow for invoking the random coding arguments [8].

4.2 Adaptive Power Allocation

In our set-up, the practical channel uncertainty model at the transmitter considers the effects of only the quantized CSI, due to the limited feedback link. We assume that the CSI is quantized by mapping the channel parameters into one of the 2^B unit-norm vectors in the codebook. Each codeword in the codebook is a randomly and independently generated unit-norm Gaussian vector. This scheme is called the Random Vector Quantization (RVQ) [27]. The legitimate receiver estimates the location of delay taps and their magnitudes perfectly, then it sends the codeword in the codebook closest to it in the Euclidean distance sense at each time instant. RVQ is employed for quantization of both magnitude of path gains and delays.

We provide two examples depicting the actual and estimated frequency responses of the channel via quantized CSI in Figures 4.2 and 4.3. The common channel parameters of the examples are as follows. There are 12 delay taps in the time domain. Frequency domain representation is obtained by using a 64 point discrete Fourier transform. Two different random vectors are generated for the gains and time delays. Path gains are i.i.d. complex Gaussian circularly symmetric random variables with zero mean and 1/2 variance for each dimension. Path delays are uniform random variables in the interval 0 to 5000ns.

Delay taps and quantized delay taps with a 5-bit RVQ and a 8-bit RVQ are shown in Figures 4.2 and 4.3, respectively. The corresponding frequency domain representations are also depicted in the same figures. Figure 4.2 shows the case where 5-bit RVQ is employed for the quantization of both the magnitude of the normalized path gain and the time delay. We observe that with the 5-bit RVQ, we can track the main changes in the spectrum, however, we cannot locate the local maxima and minima, precisely. The reconstructed channel with the 8-bit RVQ

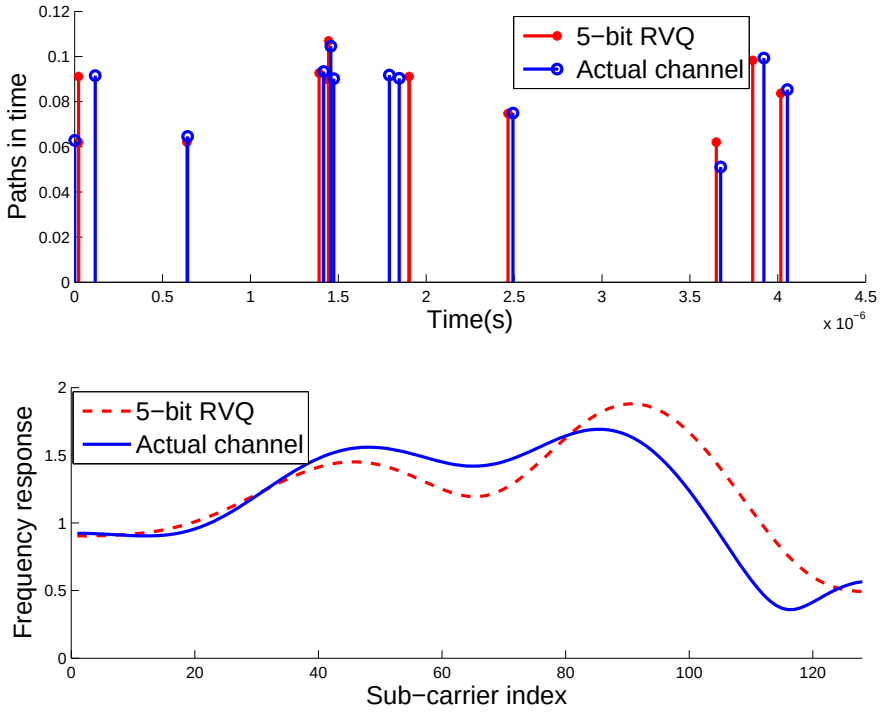

Figure 4.2: Time and frequency domain representation of both constructed version of channel using 5-bit RVQ and actual channel.

is a very good fit to the actual channel response. As expected, if the number of quantization bits is increased, the quantized channel response approximates the actual one quite well.

We use water-filling power allocation as a suboptimal strategy to analyze the effects of limited feedback link from the legitimate receiver to the transmitter. Water-filling power allocation can be written as

$$P(f) = \begin{cases} K - \frac{\phi(f)}{|H(f)|^2} & \text{, if } f \in W \\ 0 & \text{, if } f \notin W \end{cases} \tag{4.1}$$

where $P(f)$ is the distribution of the power across frequencies, $\phi(f)$ is constant for AWGN channel. W stands for bandwidth, and $H(f)$ is frequency response of channel. K is a constant to be determined based on the total power constraint.

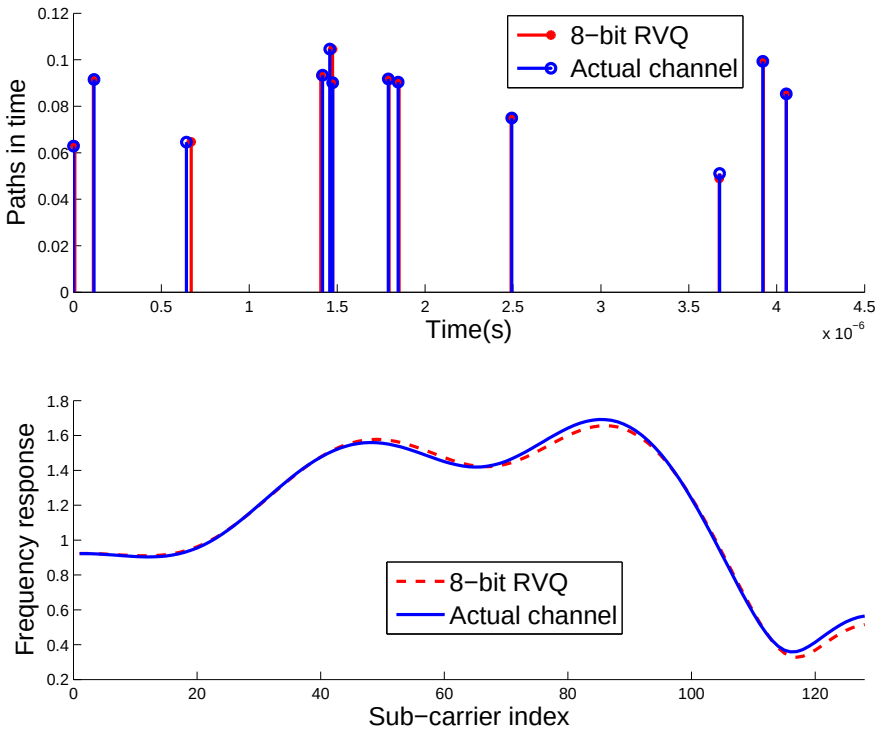

Figure 4.3: Time and frequency domain representation of both constructed version of channel using 8-bit RVQ and actual channel.

When the transmitter has quantized CSI, power allocation strategy at transmitter can be written as

$$P(f) = \begin{cases} K - \frac{\phi(f)}{\left|\hat{H}(f)\right|^2} & \text{, if } f \in W \\ 0 & \text{, if } f \notin W \end{cases} \tag{4.2}$$

where $\hat{H}(f)$ is quantized channel knowledge. The quantized version of $H(f)$ is obtained by reconstructing the channel in frequency domain by using quantized magnitudes of the delay taps and relating time delays.

We consider a frequency selective fading channel that is subdivided into N sub-channels. Bandwidth of each sub-channel is Δf and its frequency response

assumed to be flat. Then the resulting channel capacities can be written as

$$C_{Bob} \cong \sum_{i=1}^{N} log_2 \left[1 + max \left(K - \frac{\Phi_{Bi}}{\left| \hat{H}_{Bi} \right|^2}, 0 \right) \frac{|H_{Bi}|^2}{\Phi_{Bi}} \right] \tag{4.3}$$

$$C_{Eve} \cong \sum_{i=1}^{N} log_2 \left[1 + max \left(K - \frac{\Phi_{Bi}}{\left| \hat{H}_{Bi} \right|^2}, 0 \right) \frac{|H_{Ei}|^2}{\Phi_{Ei}} \right] \tag{4.4}$$

Then an achievable secrecy rate conditioned on the channel gains can be written as

$$R_{Sec} = \left[C_{Bob} - C_{Eve} \right]^+, \tag{4.5}$$

where $\hat{H}_{Bi}$ is quantized channel knowledge of i^{th} sub-channel. Fading coefficients of the channels are assumed ergodic, hence the average achievable secrecy rate can be found by taking average across time.

4.3 Numerical Examples

We use the random vector quantization under only the main channel CSIT assumption. The channel is divided into 64 sub-channels. Frequency selective fading channel is obtained by the MEDS method in [19] for each of the taps and then utilizing FFT.

In all the scenarios considered in this chapter, there is limited feedback. In other words legitimate receiver cannot send all the time domain path gains and delays accurately. Also both the SNR of the legitimate user and the eavesdropper are the same. For the first scenario whose results are shown in Figure 4.4, the channel has 12 fixed taps and relative delays are chosen uniformly in the interval 0 to 5000ns. The results are obtained after 10000 realizations for every SNR value simulated. Quantization vectors are generated randomly for every realization of both magnitude of normalized path gains and related delays.

The effects of the number of quantization bits on the achievable rates are depicted in Figure 4.4. When number of bits that are used in quantization increases,

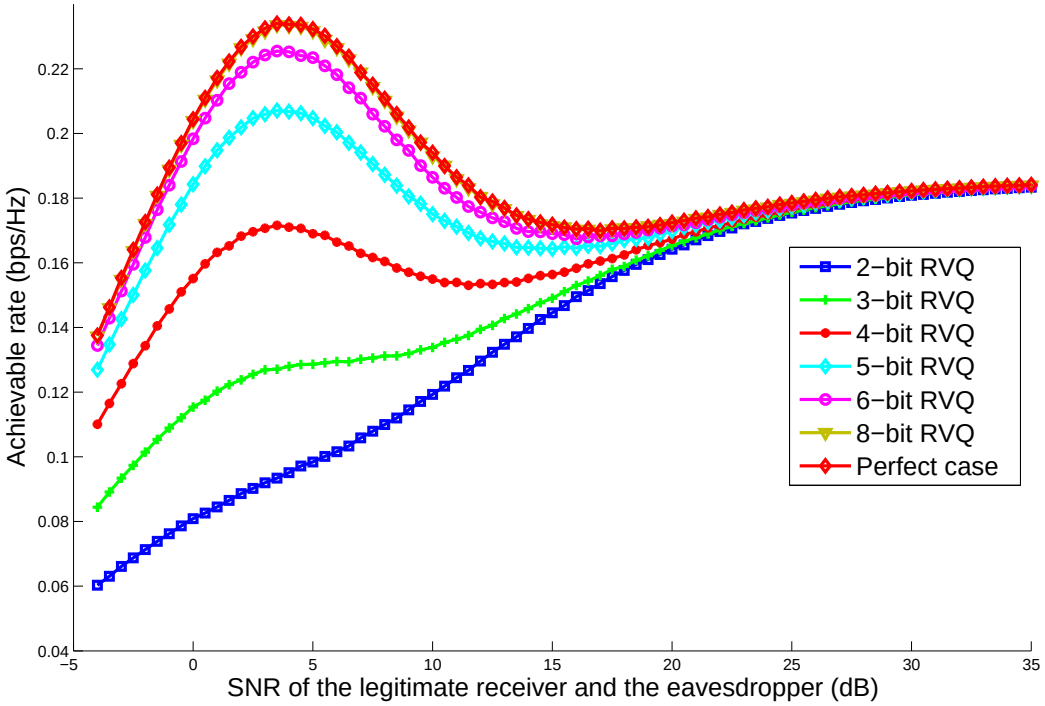

Figure 4.4: Achievable secrecy rates for different quantization levels.

the quantization error decreases and the CSI can be obtained more accurately. With 2 bit quantization, which means that 4 random vectors are generated for the normalized path gains and delays, the achievable secrecy rates are far from the perfect case in low SNRs. However, if the number of quantization levels is increased, the achievable secrecy rates approach that of the perfect channel information case. There is not much difference for high SNRs. This is because in this case, the water-filling algorithm allocates the total power almost uniformly across all the frequencies. When the number of quantization vectors is above 2^6, the achievable secrecy rate difference between the perfect case and the quantized one is negligible.

In the second scenario, the legitimate receiver can send a limited number bits for the path gains while the delays are known accurately. The receiver can choose to send path gains with higher amplitudes. That is, the gains of most powerful

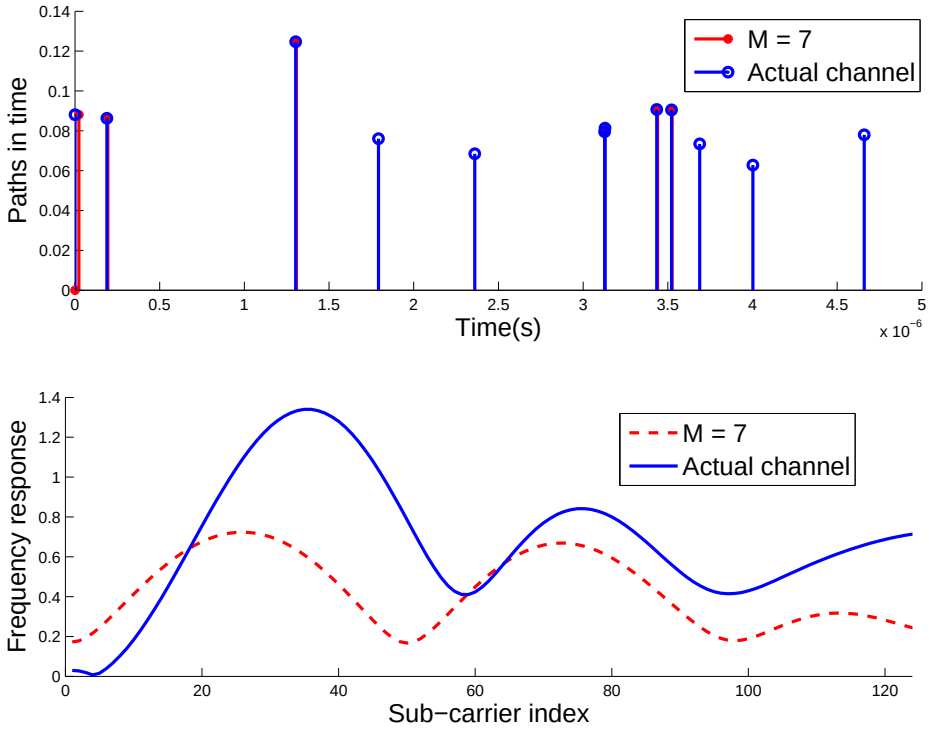

Figure 4.5: Time and frequency domain representation of both actual channel response and the constructed channel at transmitter by using 9-bit RVQ and $M = 7$.

M channel taps are quantized. The results of 10000 trials for every SNR level are obtained. B is fixed to 9 bits which means quantization vector consists of 512 elements for both real and imaginary parts of the path gains. Both main and eavesdropper channels have 12 fixed taps. The channel coefficients of eavesdropper and length are changed in every trial.

Figures 4.5 and 4.6 are examples of the estimated channels at the transmitter for different number of taps whose estimates are fed back to the transmitter. The common channel parameters of the Figures 4.5 and 4.6 are as follows. There are 12 delay taps in the time domain. Frequency response of the channel is divided into 64 sub-channels. The channel taps are i.i.d. circularly symmetric complex Gaussian random variables with zero mean and unit variance. Delays of taps

have uniform distribution in the interval from 0 to 5000ns. A 7-bit RVQ is used to construct codewords in codebook.

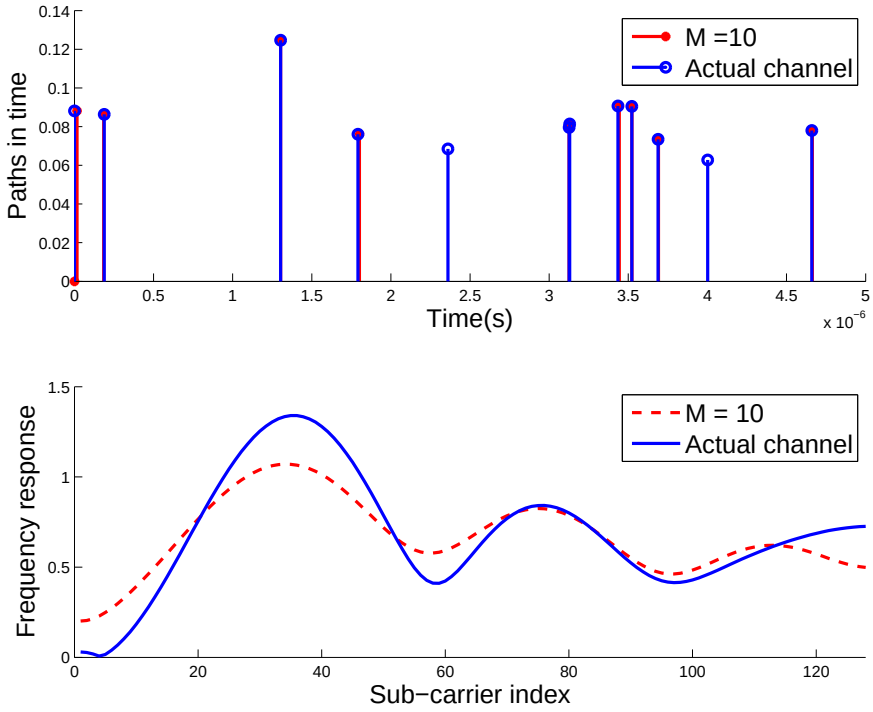

Figure 4.6: Time and frequency domain representation of both actual channel response and the constructed channel at transmitter by using 9-bit RVQ and $M = 10$.

The channel which is shown at the top of Figure 4.5 is constructed at the transmitter by using the information of 7 most powerful taps in the delay profile. The frequency response of the constructed channel is represented in the bottom of the same figure. We observe that the frequency response of the estimated channel is a good approximation to the actual case. Similarly, in the next example, we assume that the information corresponding to the most powerful 10 taps is used at the transmitter to construct the channel as depicted at the top of Figure 4.6. When $M = 10$, the frequency response of the constructed channel is very good fit to the frequency response of the actual channel.

The effects of quantizing the most significant M taps on the secrecy rates

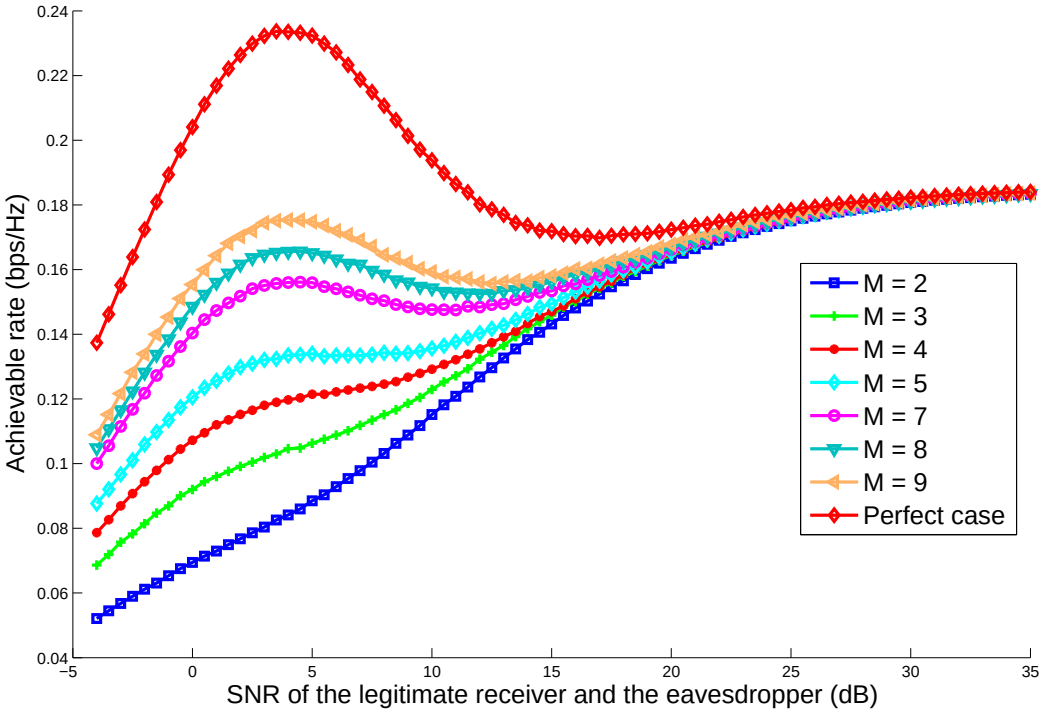

Figure 4.7: Achievable secrecy rates for different number of most powerful tap information.

are depicted in Figure 4.7. As expected, by increasing the amount of CSI, the achievable secrecy rate gets closer to the one obtained with the perfect CSI in low SNRs. In high SNRs, the quality of the CSIT does not have a considerable effect on the achievable secrecy rates. This is again due to the sub-optimality of the water-filling approach.

One final note is that these experiments clearly show that it is possible to achieve secrecy rate even if only a limited feedback channel is considered.

4.4 Chapter Summary

In this chapter, we investigated the effects of quantized CSI at the transmitter on the achievable secrecy rates over frequency selective fading channels by using random vector quantization and adaptive power allocation. We derived achievable rates for the water-filling power allocation, and provided numerical examples to study the effects of number of quantization levels on the secrecy rates. The results indicate that positive secrecy rates are achievable even in scenarios with a limited knowledge of the main channel.

Chapter 5

Conclusions

In this thesis, we investigated different power allocation strategies for maximization of secrecy rates over frequency selective fading wiretap channels with different assumptions on the transmitter side channel state information. The impact of the mobility on the achievable secrecy was analyzed and various numerical experiments were conducted to evaluate the achievable secrecy rates in different scenarios.

In Chapter 3, optimal power allocation for frequency selective fading channels was described when the channel state information of both the legitimate receiver and the eavesdropper is perfectly known at the transmitter. A low complexity power allocation scheme is proposed to reduce the implementation complexity of the optimal scheme. Proposed algorithm is found to perform 3-4 dB worse than the optimal solution. Moreover, the impacts of mobility on the secrecy rates were studied. When mobility of the legitimate receiver increases, the maximum Doppler frequency also increases, and accordingly, the channel state information which is employed by the transmitter deviates more from the actual channel conditions. Since we consider a set-up where the transmitter allocates its power by using this outdated channel state information, we observed that the achievable secrecy rates undergo a loss. Furthermore, when only the main channel is available at the transmitter, a water-filling based power allocation solution was utilized. Closed form expressions for the achievable secrecy rates were derived,

and the scheme was adopted as a suboptimal strategy. Finally, the performances with partial CSI and full CSI at transmitter were compared. The numerical results reveal that the knowledge of the eavesdropper's channel along with the main channel is crucial in obtaining high secrecy rates.

In Chapter 4, we demonstrated that taking advantage of a quantized CSI of the main channel only along with an adaptive power allocation over frequency selective fading channels lead to positive achievable secrecy rates. Numerical results were conducted with an assumption of limited feedback channel. We observed that, as expected, by increasing the number of quantization bits, the achievable secrecy rates get closer to those with a perfect feedback channel.

In this work for the scenarios where only the CSI corresponding to the main channel is available at the transmitter, we employed a water-filling power based allocation, which is indeed a suboptimal strategy as far as the maximization of the secrecy rates is concerned. Hence, a potential future work can be the investigation of optimal transmission strategies in this scenario. Furthermore, artificial noise injection along the null space of the main channel may yield better secrecy performance. As another interesting future work, one may investigate the power allocation schemes which may boost the achievable secrecy rates when the legitimate receiver and the eavesdropper both have mobility. We also note that while all the studies in this thesis was based on the Gaussian input assumption, a more practical approach can be the investigation of the limits of secure communications when the channel input is from a finite constellation.

Bibliography

[1] S. Verdu, *Foundations and Trends in Communications and Information Theory*. Now Publishers, first ed., 2008.

[2] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical layer secrecy in multi antenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29 – 40, Sep. 2013.

[3] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2470 – 2492, June 2008.

[4] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J*, vol. 28, pp. 656 – 715, Oct. 1949.

[5] A. Wyner, "The wiretap channel," *Bell Syst. Tech. J*, vol. 54, no. 8, pp. 1355 – 1387, Oct. 1975.

[6] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 54, pp. 339 – 348, May 1978.

[7] S. K. Leung-Yan-Cheong and M. Hellman, "The gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451 – 456, July 1978.

[8] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy of capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687 – 4698, Oct. 2008.

[9] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *IEEE International Symposium on Information Theory*, (Seattle, WA, USA), pp. 356 – 360, July 2006.

[10] Z. Li, R.Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *IEEE International Symposium on Information Theory*, (Nice), pp. 1296 – 1300, June 2007.

[11] M. Kobayashi and M. Debbah, "On the secrecy capacity of frequencyselective fading channels: A practical Vandermonde precoding," in *PIMRC. IEEE 19th International Symposium*, (Cannes), pp. 1–5, Sept. 2008.

[12] F. Renna, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1354 – 1367, Aug. 2012.

[13] G. E. and A. H., "Secure communication in frequency selective channels with fade-avoiding subchannel usage," in *Communications Workshops (ICC), 2014 IEEE International Conference*, (Sydney, NSW), pp. 813 – 818, June 2014.

[14] M. Shankar, *Introduction to Wireless Systems*. John Wiley and Sons Inc, first ed., 2002.

[15] R. W. Chang, "Synthesis of band-limited orthogonal signals for multichannel data transmission," *Bell Syst. Tech. J*, vol. 45, pp. 1775 – 1796, Dec. 1966.

[16] S. Boyd and L. Vandenberghe, *Convex Optimization*. London, U.K.: Cambridge Univ. Press, seven ed., 2004.

[17] Z. Li, R. Yates, and W. Trappe, *Securing Wireless Communications at the Phsical Layer*. Springer US, first ed., 2006.

[18] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas - part II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515 – 5532, Nov. 2010.

[19] C.-X. Wang and M. Patzold, "Methods of generating multiple uncorrelated rayleigh fading processes," in *Proc. 57th IEEE Vehicular Technology Conference, IEEE VTC 2003 - Spring*, pp. 510–514, April 2003.

[20] T. M. Cover and J. A. Thomas, *Elements of. Information Theory*. Wiley, second ed., 1991.

[21] J. G. Proakis, *Digital Communications*. New York: Mc Graw-Hill, third ed., 1995.

[22] S. M.R. and P. R.L., "Adaptive modulation with imperfect channel information in OFDM," in *ICC 2001 IEEE International Conference*, vol. 6, (Helsinki), pp. 1861 – 1865, June 2001.

[23] N. Laurenti and H. V. Poor, "Physical-layer secrecy for OFDM transmissions, over fading channels," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1354 – 1367, August 2012.

[24] Z. Zhou, "Capacity variance of OFDM systems over time and frequency selective fading channels," in *Electrical and Control Engineering (ICECE), 2011 International Conference*, (Yichang), pp. 2920 – 2923, Sept. 2011.

[25] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*. Academic Press, seventh ed., 2007.

[26] A. B.-S. D. Falconer, S. L. Ariyavisitakul and B. Eidson, "Frequency domain equalization for single-carrier broadband wireless systems," *IEEE Communications Magazine*, vol. 40, no. 4, pp. 58 – 66, Apr. 2002.

[27] W. Santipach and M. L. Honig, "Asymptotic performance of MIMO wireless channels with limited feedback," in *2003 IEEE Military Commun. Conf.*, vol. 1, (Boston, MA, USA), pp. 141 – 146, Oct. 2003.