PHYSICAL LAYER SECURITY SCHEMES FOR WIRELESS COMMUNICATION SYSTEMS

A THESIS SUBMITTED TO

THE GRADUATE SCHOOL OF

ENGINEERING AND NATURAL SCIENCES

OF ISTANBUL MEDIPOL UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR

THE DEGREE OF

MASTER OF SCIENCE

IN

ELECTRICAL, ELECTRONICS ENGINEERING AND CYBER SYSTEMS

By

Marwan Yusuf

August, 2016

ABSTRACT

PHYSICAL LAYER SECURITY SCHEMES FOR WIRELESS COMMUNICATION SYSTEMS

Marwan Yusuf

M.S. in Electrical, Electronics Engineering and Cyber Systems

Advisor: Prof. Dr. Hüseyin Arslan

August, 2016

Security in wireless communications has always been a major concern due to the broadcast nature of the radio waves. Apart from the conventional cryptologic methods that are performed in the upper layers, physical-layer security is emerging as a promising paradigm that aims to take advantage of the random propagation characteristics of wireless channels. For the rich multipath environment, we propose a technique that exploits the inter-carrier interference, caused by a carrier frequency offset in OFDM systems, to degrade the performance of eavesdroppers. The proposed technique is based on introducing a controlled interference to pre-compensate the effect of the carrier offset only for the legitimate user in time division duplex systems. Frequency division duplex is a more challenging scenario in terms of security aspects due to the channel state information (CSI) leakage problem. We propose another technique that uses the conventional scheme of performing CSI feedback. We enhance the security of OFDM systems in frequency selective fading channels by using signal space diversity (SSD). By adapting the interleaving pattern used in SSD to the channel response of the legitimate user, more diversity gain is provided to the legitimate user compared to an eavesdropper. The smart adaptation of the interleaving pattern reduces both: the computational complexity and the diversity gain delivered to an eavesdropper compared to the conventional SSD system. For open environment, where scatterers are limited or line-of-sight dominates the communication, we introduce a complementary scheme that uses a multiple antenna technique called directional modulation in a coordinated multi-point system to provide location-specific secure transmission to legitimate users. We characterize the performance achievable using a newly defined metric called clear region. Finally we investigate the effect of the number of antennas and modulation order on the performance.

Keywords: Wireless, Physical Layer, Security, Eavesdropping, OFDM.

ÖZET

KABLOSUZ HABERLEŞME SİSTEMLERİ İÇİN FİZİKSEL KATMAN GÜVENLİĞİ ŞEMALARI

Marwan Yusuf

Elektrik, Elektronik Mühendisliği ve Siber Sistemler, Yüksek Lisans

Tez Danışmanı: Prof. Dr. Hüseyin Arslan

Ağustos, 2016

Radyo dalgalarının havada yayılımından dolayı, kablosuz haberleşmede güvenlik her zaman temel bir sorun olmuştur. Üst katmanlarda uygulanan alışagelmiş kripto yöntemlerinden farklı olarak fiziksel katman güvenliği, kablosuz haberleşme kanallarının rastgele yayılım karakteristiklerinden yararlanmayı amaçlamaktadır. Bu çalışmada, zengin çoklu yol ortamları düşünülerek, gizli dinleyicilerin performanslarını düşürmek amacıyla, OFDM sistemlerindeki taşıyıcı frekans kaymasından kaynaklanan taşıyıcılar arası girişimi kullanan bir teknik sunulmuştur. Bu teknik, zaman bölmeli dubleks sistemlerde sadece meşru kullanıcı için, taşıyıcı kayması etkisini önceden dengeleyen kontrol edilebilir bir girişimin tanıtılmasına dayanmaktadır. Kanal durum bilgisi (CSI) sızma probleminden kaynaklanan güvenlik durumları temel alındığında, frekans bölmeli dubleks yöntemler daha zorlayıcı senaryolardır. CSI geri bildirimini kullanan alışagelmiş şemaları kullanan bir teknik de sunulmuştur. İşaret uzayı çeşitliliği (SSD) kullanılarak frekans seçici sönümlemeli kanallarda OFDM sistemlerinin güvenliği arttırılmıştır. Meşru kullanıcının kanal cevabında SSD için kullanılan serpiştirme örüntüsü uyarlanarak, gizli dinleyicilere kıyasla meşru kullanıcı için daha fazla çeşitlilik kazanılmıştır. Serpiştirme örüntüsünün akıllıca uyarlanmasıyla hesaplama karmaşıklığı ve gizli kullanıcıya ulaştırılan çeşitlilik kazancı bu sayede azaltılmıştır. Yansıtıcıların az ve açık görüş hattının baskın olduğu açık bir çevredeki haberleşme için, çoklu antenlerin kullanıldığı tamamlayıcı bir şema tanıtılmıştır. Koordineli çoklu nokta sistemlerinde yönlü modülasyon olarak adlandırılan bu yöntem, meşru kullanıcılar için konum tabanlı güvenli iletişim sağlamaktadır. Ayrıca, yeni önerilen bir ölçev olan temiz bölge, performans karakteristikleri açısından incelenmiştir. Performans açısından anten sayısının ve modülasyon derecesinin etkileri incelenmiştir.

Anahtar sözcükler: Kablosuz, Fiziksel Katman, Güvenlik, Gizli Dinleme, OFDM.

To my family.

Acknowledgement

First, I would like to thank my advisor Dr. Hüseyin Arslan for his guidance, encouragement and support throughout my study. I wish to thank Dr. Tunçer Baykaş and Dr. M. Kemal Özdemir for serving on my committee and for offering valuable suggestions.

It has been a privilege to join the Communication, Signal processing and Networking Center (CoSiNC). I would like to thank my friends Moustafa Ibrahim, Morteza Soltani, Jehad Hamamreh, Moustafa Helmy and Murat Karabacak from our research group for their support as friends and for sharing their knowledge as colleagues. Special thanks to Morteza Soltani for his continuous support and fruitful discussions during my master period.

Last but by no means least, I would like to thank my parents for their continued support, encouragement and sacrifice throughout the years, and I will be forever indebted to them for all that they have done.

Contents

List of Figures

Chapter 1

Introduction

Wireless communications have become indispensable for providing seamless, mobile , and broadband data transfer. However, the broadcast nature of radio waves results in a critical drawback in terms of transmission security and privacy, especially for applications in vital domains such as military, public safety or health care. Adversaries can possibly intercept the data traffic as long as they lie within the radio transmission coverage areas, a security problem known as eavesdropping. Conventionally, these issues have been addressed in the upper layers of the network protocol stack using cryptography-based solutions, which typically rely on the use of confidential secret keys to seal the transmitted messages. However, with the rapid growth of the number of wireless devices, the secret key distribution and management that are required to maintain these operations are becoming increasingly difficult, and are introducing larger overhead and latency to the system. Besides the requirement of a pre-shared key; encryption does not prevent an eavesdropper from capturing the information signal, but only makes its job harder when it runs an offline exhaustive key search, which is also known as a brute-force attack. In order to make the signal meaningless for eavesdroppers in the lowest layer possible, physical-layer security is emerging as a good paradigm due to its ability to ensure communication secrecy without the explicit use of secret keys. It serves as a promising technique for highly dynamic or ad-hoc systems such as device-to-device and machine-type communication systems.
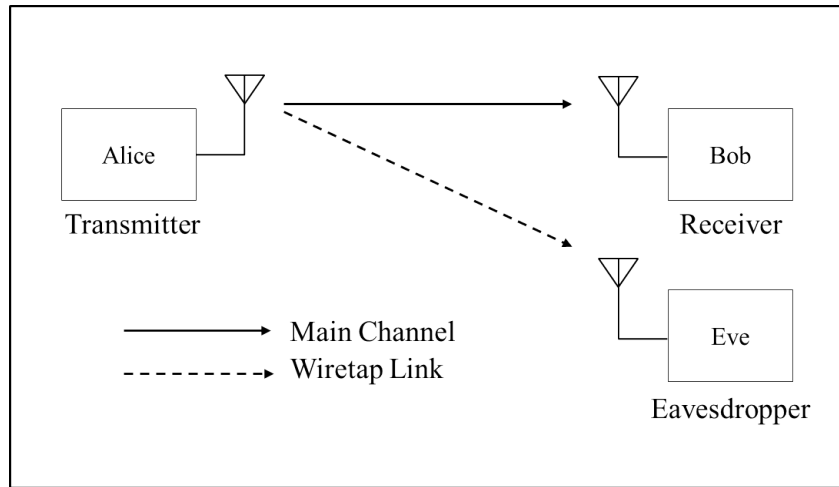
Figure 1.1: A wireless communication scenario consisting of a transmitter and a legitimate receiver in the presence of an eavesdropper.

The basic secret communication system, often referred to as the wiretap channel in the information theory literature, consists of three terminals: a transmitter (Alice), a legitimate receiver (Bob), and an eavesdropper (Eve), as illustrated in Fig.1.1. Wyner has the pioneer work for physical layer security in [1], where he studied securing communications for a discrete memoryless wiretap channel. In [2], The results obtained by Wyner were extended to the Gaussian wiretap channel. In that work, the secrecy capacity was developed as the difference between the channel capacity of the main link and that of the wiretap link. Once the secrecy capacity falls below zero, the security of transmission from source to destination is lost, and the eavesdropper can successfully intercept the transmission. In order to improve transmission security against eavesdropping attacks, it is of great importance to increase the secrecy capacity, so as to reduce the probability of occurrence of an intercept event. For the fading effect in wireless communications, which is the main physical layer parameter in our work, optimal power allocation with full CSI is given for slow fading channels in [3]. Hence, recent information-theoretic studies of the wiretap channel have demonstrated the possibility of achieving secrecy in the physical layer with the sole use of channel coding and signal processing techniques.

To that end, practical approaches have been investigated that make use of the random multipath propagation environment, multiple degrees of input/output or

2

flexible waveform designs. In this work, we propose several secure communication methods that exploit the randomness and uniqueness of the wireless channel between the transmitter and receiver for time varying and multipath fading environments for SISO and MISO scenarios. By considering the channel spatial dependency, meaning that wireless channels associated with different endpoints at separate locations typically exhibit uncorrelated propagation characteristics in rich scattering environments, our aim is to have a transmission scheme where the information only becomes meaningful inside a desired geographical location. Thus, any receiver located outside of the intended location will be disabled from capturing private and sensitive information.

Orthogonal Frequency Division Multiplexing (OFDM) has been widely adopted in modern wireless systems. Its advantages include high spectral efficiency and robustness against multipath fading. On the other hand, due to its distinct time and frequency characteristics, a conventional OFDM signal is vulnerable to eavesdropping [5]. In Chapter 2[1], we take advantage of one of the drawbacks of OFDM for security purposes. The performance of OFDM is very sensitive to frequency synchronization errors. We exploit the channel reciprocity in a time division duplex (TDD) system to introduce self-interference that cancels the effect of the inter-carrier interference caused by a carrier frequency offset (CFO) between Alice and Bob. This pre-compensation process depends on both the channel response and the local CFO of Bob. Hence, under the assumption that Eve experiences an uncorrelated channel response, its performance is expected to be degraded.

A more challenging scenario, in term of security aspects, is the frequency division duplex system. In such scenario, the knowledge of CSI cannot be estimated independently at both Alice and Bob, as in the TDD case. A feedback link is required to share the unique CSI estimated at Bob with Alice. However, since this feedback link is accessible by Eve as well, the CSI is no longer a secret, which is known as the CSI leakage problem. In Chapter 3[2], we propose a technique that uses the conventional scheme of performing CSI feedback and thus can be viewed as a worst-case-scenario technique where CSI of both the main and the wiretap channels are available at Eve

---

[1]This work is published in [35].
[2]This work is published in [36].

[6]. The technique uses diversity to provide more gain to Bob compared to Eve. Diversity, originally used to mitigate the performance degradation on fading channels and increase transmission reliability, is also used to improve the security of wireless transmission [7]. Several types of diversities are used in the literature such as space diversity, cooperative diversity or frequency diversity. Another type of diversity which has not received that much attention is signal space diversity. It can provide performance improvement over fading channels without using extra bandwidth and power consumption, by taking advantage of the inherent orthogonality in the signal space [8, 9]. By making use of the OFDM performance in frequency-selective channels, an adaptive interleaving design is proposed to maximize the diversity gain of Bob based on his channel. Since the signal received by Eve is passing through different channel, the gain delivered is less significant compared to Bob.

So far we have used the uncorrelation property provided by the rich scattering environments to secure transmission. However, for open environments, where scatterers are limited or line-of-sight (LOS) dominates the communication, other techniques are needed. This problem has been conventionally addressed using multiple antenna techniques and one technique that has been recently developed for secure transmission is Directional Modulation (DM) [10, 11]. Unlike the conventional beamforming, where same information is transmitted to all directions, DM transmits the desired data in the direction of legitimate user and randomizes the field pattern in all other directions. An obvious drawback of this scheme is that any receiver along the information beam can easily intercept the signal. In Chapter 4[3], we propose a scheme that overcomes this scenario by using DM in a coordinated multipoint (CoMP) system to provide a location-specific secure transmission to legitimate users. We characterize the performance achievable using a newly defined metric called Clear Region (CR) that refers to the area within which a receiver can access and decode the signal being transmitted.

---

[3]This work is published in [37].

4

1.1 Organization of Thesis

The thesis consists of 5 chapters. An overview of OFDM system is provided in Chapter 2. The effect of CFO and the security technique developed to make use of it are also analyzed in terms of secrecy capacity and power considerations. Chapter 3 briefly introduces SSD system along with the proposed technique to enhance the security of OFDM. Adaptive interleaving design is proposed and simulation results are given at the end of the chapter. In Chapter 4, a brief overview to DM and the proposed CoMP system is provided, followed by the investigation of the CR metric and the effect of the number of antennas and modulation order on the performance. Finally, Chapter 5 concludes the thesis with a summary discussion.

Chapter 2

Controlled Inter-carrier Interference for Securing OFDM Systems

2.1 Introduction

Multicarrier modulation corresponds to the use of different frequencies for the transmission of multiple data streams. Instead of sending the information back to back in a serial manner, multiple symbols are transmitted simultaneously in parallel. A special case of multicarrier transmission, orthogonal frequency division multiplexing, has been widely employed in modern wireless systems because of its high spectral efficiency and robustness against multipath fading. It can achieve high scalable data rates with achievable complexity.

On the other hand, a conventional OFDM signal is vulnerable to eavesdropping due to its distinct time and frequency characteristics [5]. As a result, eavesdroppers can blindly estimate the transmission parameters and intercept the transmitted information of OFDM systems. Hence, it is of practical interest to enhance the built-in security of OFDM systems. In the literature, various techniques were developed to

achieve transmission level security and covertness in OFDM systems. In [12], cyclic prefix and pilot tones are removed to suppress OFDM features, and inter symbol interference (ISI) is cancelled using a decision feed-back equalizer (DFE) and preambles are replaced by pseudo- random sequences in order to facilitate time and frequency synchronization. A random frequency offset is added to each preamble to further mask the spectral lines. This has the obvious disadvantage of increasing receiver complexity which eliminates the advantage of OFDM in handling multipath fading channel by using Cyclic Prefix (CP), alongside with the possible error propagation between OFDM symbols due to the DFE. Alternatively, cyclic features are concealed by changing the CP selection region for each symbol [13] or by inserting random data between OFDM symbols [14] in a pseudo-random fashion. Also, CP length variation according to the maximum excess delay of the channel is offered as an extra precaution. However, these techniques require spectral redundancy either by using longer CP than needed or using irrelevant data.

In this chapter, we exploit one of the known drawbacks of OFDM for security purposes. The performance of OFDM is very sensitive to frequency synchronization errors. The existence of a carrier frequency offset between the transmitter and the receiver is mainly due to oscillator instabilities or Doppler shifts. The resulting inter-carrier interference (ICI) degrades the system performance [15] since the transmitted information cannot be retrieved error-free even in the absence of noise. Also, CFO may cause the loss of orthogonality among subcarriers. There have been several papers on the subject of synchronization in recent years especially in the crucial case of uplink in OFDMA systems. One of the most robust synchronization methods can be found in [16]. Two main approaches can be used to mitigate the frequency offset in the uplink of OFDMA systems. In the first one, which is called the feedback method, the estimated frequency offset values at the base station are fed back to the users on a control channel so that they can adjust their transmission parameters [17]. The obvious disadvantage of this approach is the need for the control channel. In the second approach, namely the compensation method [18, 19], users do not change their transmission parameters. Instead, the base station compensates for the frequency offsets of all users by employing signal processing techniques without the need for a control channel.

This chapter is organized as follows: a brief OFDM system modeling is presented followed by an explanation of the inter-carrier interference caused by carrier frequency offset. Then the proposed technique is presented which uses carrier offset pre-compensation for security. Finally, simulation results are given for secrecy evaluation along with power considerations.

2.2   System Model

2.2.1   OFDM System Model

In OFDM the bit stream is mapped to symbols that modulate a series of subcarriers, each separated by a spacing of $1/T$ in frequency domain, where T is the symbol duration. Even though the modulated symbols spectrally overlap, they are orthogonal to each other. This modulation process can be computed efficiently by applying the N-point Inverse Fast Fourier Transform (IFFT) to each OFDM block to obtain the time domain signal. The transmitted modulated signal sampled in time domain is given by

$$x_l(n) = \sum_{k=0}^{N-1} X_l(k)e^{j2\pi kn/N} \tag{2.1}$$

where $X_l(k)$ denotes the symbol at the kth subcarrier in the lth OFDM symbol and N is the number of subcarriers. To overcome the multipath fading channel, a guard interval is appended at the front of each OFDM symbol. This guard interval is usually inserted by extending the OFDM symbol with a CP that allows for both the removal of ISI and maintaining subcarriers orthogonality. Hence, after the removal of this extension at the receiver, the signal is ISI-free and each subcarrier channel response is considered as a flat fading channel. Let $y(n)$ be the received signal

$$y(n) = \sum_{m=0}^{M-1} h(m)x(n-m) + z(n) \tag{2.2}$$

where $h(m)$ is the channel response with M taps and $z(n)$ is the sampled Additive White Gaussian Noise (AWGN) in time domain. The received symbols in frequency

domain can be represented in a matrix form as

$$\mathbf{y} = \mathbf{FTH_tGF^{-1}x} + \mathbf{z} \tag{2.3}$$

where $\mathbf{y}$ is the received symbols vector, $\mathbf{T}$ is the truncating matrix for CP removal, $\mathbf{H_t}$ is the matrix with channel impulse responses, $\mathbf{G}$ is the matrix for CP inserting, $\mathbf{F}$ and $\mathbf{F^{-1}}$ are the FFT and IFFT matrices, $\mathbf{x}$ is the vector of transmitted symbols and $\mathbf{z}$ is the noise vector in frequency domain. Assuming the CP length is greater than maximum delay spread, $\mathbf{TH_tG}$ is a circular square matrix and can be modeled as

$$\mathbf{TH_tG} = \mathbf{F^{-1}H_fF} \tag{2.4}$$

where $\mathbf{H_f}$ is the diagonal matrix of the channel frequency response. Then the received signal can be simplified into

$$\mathbf{y} = \mathbf{H_fx} + \mathbf{z} \tag{2.5}$$

2.2.2 Inter-carrier Interference Caused by Carrier Frequency Offset

Let us consider the case where we have a carrier offset between the transmitter and the receiver. Assuming perfect time synchronization, the received symbols after FFT can be written as

$$Y_l(k) = \sum_{n=0}^{N-1} y_l(n) e^{-j2\pi(k+\epsilon)n/N} \tag{2.6}$$

$$= \sum_{k'=0}^{N-1} X_l(k') H(k') I(k, k', \epsilon) \tag{2.7}$$

where $\epsilon = \Delta f T$ is the CFO, which represents the frequency offset Δf normalized to the carrier spacing $1/T$ and $H(k')$ is the flat channel response at the k'^{th} subcarrier. The spectral leakage I among subcarriers is defined as [15]

$$I(k, k', \epsilon) = e^{j\pi(k-k'+\epsilon)\frac{N-1}{N}} \frac{\sin(\pi(k-k'+\epsilon))}{N\sin(\frac{\pi(k-k'+\epsilon)}{N})} \tag{2.8}$$

$I(k, k', \epsilon)$ can be interpreted as the normalized interference on the k'^{th} subcarrier from the kth subcarrier. For a large number of subcarriers N, the normalized interference power can be approximated by

$$|I(k, k', \epsilon)|^2 = \left| \frac{\sin(\pi(k - k' + \epsilon))}{\pi(k - k' + \epsilon)} \right|^2 \tag{2.9}$$

Note that the orthogonality among subcarriers is destroyed when ϵ is not an integer. In other words, to have ICI, the induced carrier offset should be a fractional multiple of the carrier spacing. Fig.2.1 shows the increase of interference power among subcarriers as the fractional frequency offset (FFO) increases. As shown in (2.6) the effect of carrier offset on the time domain signal is a phase shift that is proportional to the FFO ϵ and time index n, so it can be written as

$$\mathbf{y} = \mathbf{FEF^{-1}}(\mathbf{H_f x} + \mathbf{z}) = \mathbf{E_c H_f x} + \mathbf{z}' \tag{2.10}$$

where $\mathbf{E}$ is a diagonal matrix given by $\mathrm{diag}[1\ e^{j2\pi\epsilon/N}... e^{j2\pi\epsilon(N-1)/N}]$ and $\mathbf{E_c} = \mathbf{FEF^{-1}}$ is the interference matrix that models the same effect as a circular convolution in the frequency domain [19]. $\mathbf{E_c}$ is basically the effect of the ICI given in (2.8).
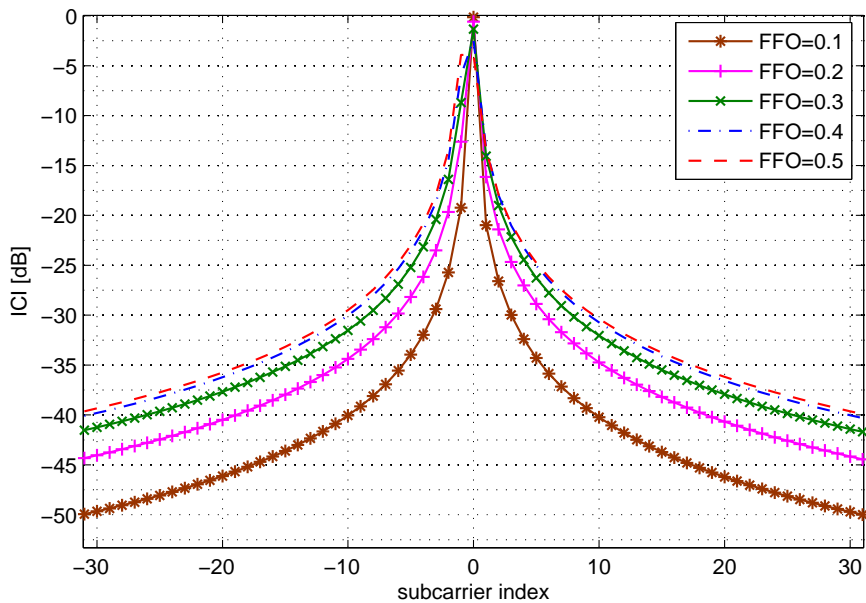

Figure 2.1: The interference power at each carrier index for various fractional offset values.

2.3 Securing Communication via Carrier Offset Pre-compensation

We consider a time-division duplexing system where we can exploit the reciprocity of the channel. In this system, Bob sends his signal with an induced CFO that Alice can estimate and compensate using the compensation method mentioned earlier. With the channel state information known to Alice, she will transmit her data with the carrier offset pre-compensated in such a way that, when it passes through Bob's channel, it is received without ICI. This is different from just having a CFO at Alice because the pre-compensation process depends also on the channel between Alice and Bob. Even if Eve manages to blindly estimate the offset, she will still suffer from degradation due to the uncorrelation between her channel and Bobs channel. In other words, the pre-compensation acts as a pre-equalizer, not to the channel but to the ICI with respect to Bob's channel. To further increase the security of communication, Bob can change the offset continuously, hence both CFO and CSI need to be tracked by Alice. This makes the estimation and tracking done by Eve a difficult task, even if she uses a very complex algorithm to compensate what is done at Alice. Also the simple structure of the proposed scheme shown in Fig.2.2, with only a carrier offset at the receiver and shifting the complexity to transmitter, allows it to be suitable for future low power demands of green radios.
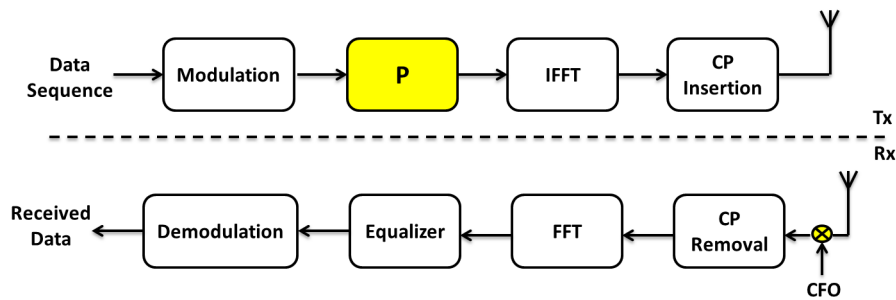

Figure 2.2: Block Diagram of the proposed secure OFDM system over main channel.

For the proposed scheme, the transmitted symbols from Alice are first passed

11

through a pre-compensation stage before IFFT as shown in Fig.2.2. This pre-compensation matrix P is generated such that the effect of ICI is eliminated at Bob. Disregarding the noise, the pre-compensation matrix generation is done by setting the received signal as following

$$\mathbf{y_B} = \mathbf{E_c}\mathbf{H_f}\mathbf{P}\mathbf{x} = \mathbf{H_f}\mathbf{x} \tag{2.11}$$

$$\mathbf{P} = \mathbf{H_f^{-1}}\mathbf{E_c^{-1}}\mathbf{H_f} \tag{2.12}$$

where $\mathbf{E_c^{-1}} = \mathbf{F^{-1}}\mathbf{E^{-1}}\mathbf{F}$. Hence, $\mathbf{P}$ can be generated from the channel frequency response and the carrier offset both estimated at Alice. This process, which we may call as interference zero-forcing, is not computationally complex, since both matrices $\mathbf{E^{-1}}$ and $\mathbf{H_f^{-1}}$ are diagonal ones. For the case of Eve, the received signal will be

$$\mathbf{y_E} = \mathbf{E_E}\mathbf{H_E}\mathbf{H_f^{-1}}\mathbf{E_c^{-1}}\mathbf{H_f}\mathbf{x} + \mathbf{z_E} \tag{2.13}$$

where a different frequency offset gives the ICI matrix $\mathbf{E_E}$ and $\mathbf{H_E}$ is the frequency channel response of Eve. Because the channels of Bob and Eve are uncorrelated, it is hard to eliminate the effect of the ICI induced by the pre-compensation stage. Even if Eve manages to get the right offset, the channel to be estimated is no longer flat as shown in (2.13). The estimation of the diagonal and off diagonal elements becomes a tedious process for Eve. By rapidly varying the offset value at Bob, this estimation process will even be more difficult, if not impossible. It will be shown in the simulation results that, with the same offset value as Bob, Eve still suffers from performance degradation since the channel estimation assumes flat fading for each subcarrier.

2.4 Secrecy Evaluation

To measure the secrecy performance of the proposed scheme, we refer to the information-theoretic metrics usually used for characterizing the security level of a communication link, in our case a fading wire-tap channel [20]. We define the achievable secrecy rate as

$$R_s = R_B - R_E \tag{2.14}$$

12

where R_B and R_E are the achievable rates of Bob and Eve respectively. For an OFDM system with N subcarriers, the rate is given by the summation of the rates of each individual subchannel

$$R = \sum_{k=1}^{N} \log_2(1 + \text{SINR}(k)) \tag{2.15}$$

where $\text{SINR}(k)$ is the signal to interference plus noise ratio of the kth subchannel. Hence, for Bob's channel

$$\text{SINR}_B(k) = \frac{|H(k)|^2}{N_B} P_t \tag{2.16}$$

where N_B is noise power at Bob and P_t is the transmitted signal power. Note that there is no interference component, since the carrier offset is pre-compensated for the channel of Bob according to (2.11). On the other hand, for the case of Eve

$$\text{SINR}_E(k) = \frac{|q_k(k)|^2 P_t}{\sum_{k' \neq k}^{N} |q_{k'}(k)|^2 + N_E} \tag{2.17}$$

where $[q_1(k)\ q_2(k)..\ q_N(k)]$ is the kth row of Eve's interference matrix given from (2.13) by $\mathbf{Q} = \mathbf{E_E H_E P}$. Hence, the secrecy rate can be rewritten as

$$R_s = \sum_{k=1}^{N} \log_2 \left(\frac{1 + P_t|H(k)|^2/N_B}{1 + P_t|q_k(k)|^2/\left(\sum_{k' \neq k}^{N} |q_{k'}(k)|^2 + N_E\right)} \right) \tag{2.18}$$

2.5   Simulations

2.5.1   Performance Analysis

To verify the performance of the proposed transceiver structure with carrier offset pre-compensation, we simulate an OFDM system of 64 subcarriers and QPSK modulation with a multi-tap channel model of Rayleigh fading distribution. The power delay profile is a normalized 8-tap exponentially decaying profile with a delay spread smaller than the CP. First, we assume perfect channel and offset estimation, then we show in our simulations that the effect of the estimation error will just introduce some noise floor to the receiver. Also we assume a conventional receiver for Eve, that is,
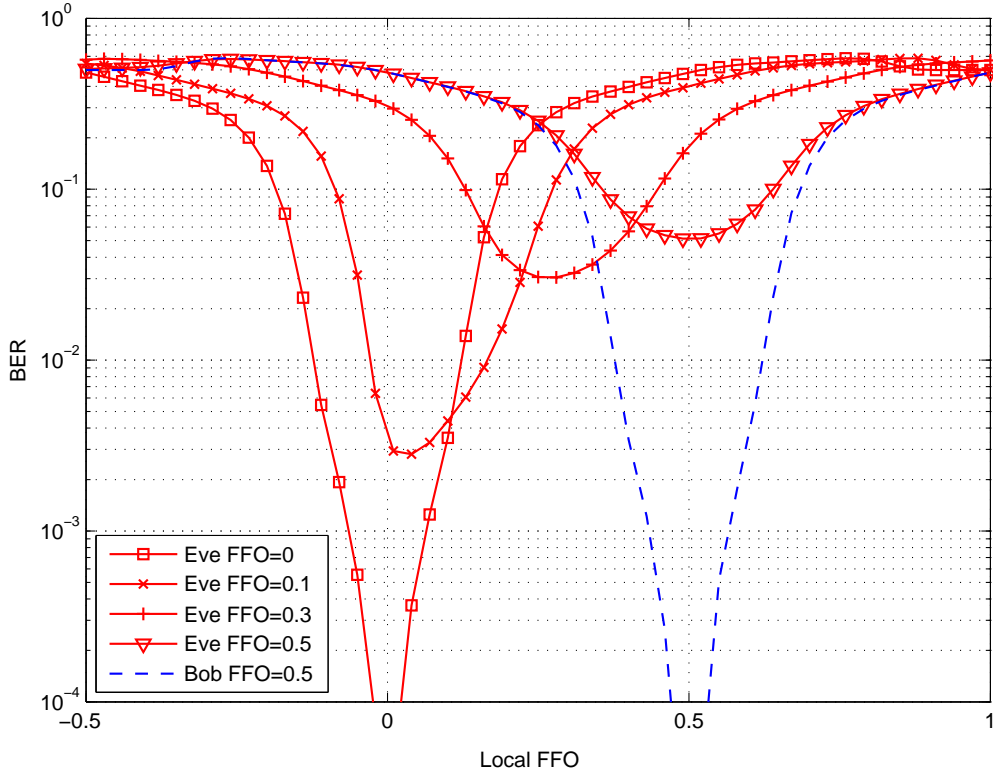
Figure 2.3: BER vs. local carrier offset FFO for Bob (blue) and Eve (red) at different pre-compensated FFO values.

a receiver that tries to compensate the frequency offset and estimate the one-tap channel based on the received signal.

First, we test for the fading channel without any noise. Fig.2.3 shows the Bit Error Rate (BER) vs. the local carrier offset at different pre-compensated FFO values. It shows the degradation of Eve's performance as the offset value increases. On the other hand, Bob receives the data error-free when the local offset is the same as the pre-compensated value. This is the case when there is no mismatch in the offset estimation between transmitter and receiver. In case of an estimation error, some BER will start to appear as shown by the V-shaped performance of FFO = 0.5 for Bob. Note that Eve has the same V-shaped performance at FFO = 0. Since this security scheme depends on the self-ICI induced, the best case is for FFO = 0.5 which gives the largest spectral leakages among subcarriers. It is clear that, with the same

14
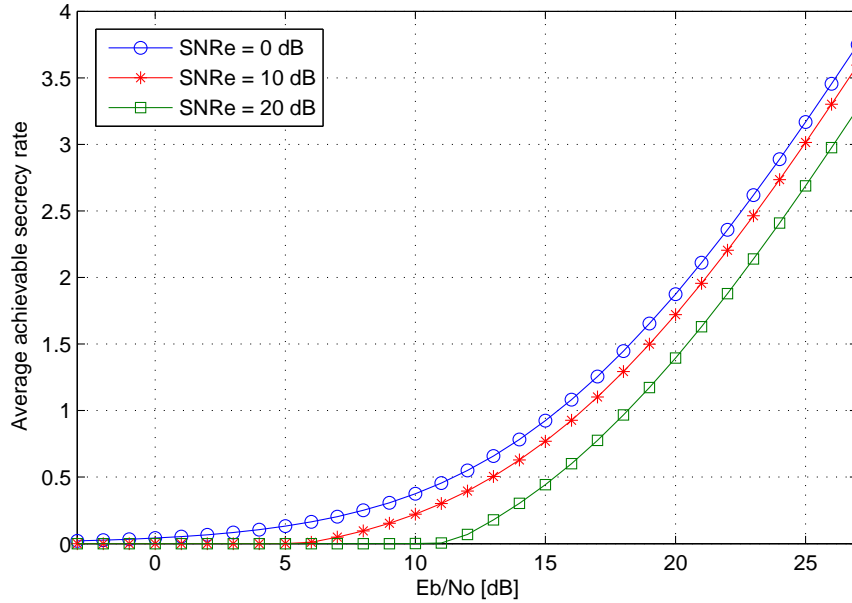
Figure 2.4: The change of the average achievable secrecy rate per subchannel with respect to Eb/No of Bob's channel at FFO=0.5.

FFO value as Bob, Eve still suffers from performance

For evaluating the secrecy performance, we calculate the average achievable secrecy rate per subchannel for different Eb/No values at Bob. Fig.2.4 shows the change of the achievable secrecy rate with the change of the signal-to-noise ratio (SNR) of Eve's channel for the largest pre-compensated FFO of 0.5. Since we want to measure the performance of our scheme, we added the noise to Eve's channel based on the signal power without the interference component. That is why we plot the rate at different SNR, not SINR for Eve. It is clear that we can achieve a positive secrecy rate even when the SNR at Bob is lower than that at Eve.

2.5.2 Power Considerations

We now take a look at the power aspects of this technique. The transmitted power is expected to increase as a function of the FFO until we reach 0.5, due to the pre-compensation stage. Also the Peak to Average Power Ratio (PAPR) is a crucial

Figure 2.5: PAPR distribution at different pre-compensated FFO values.
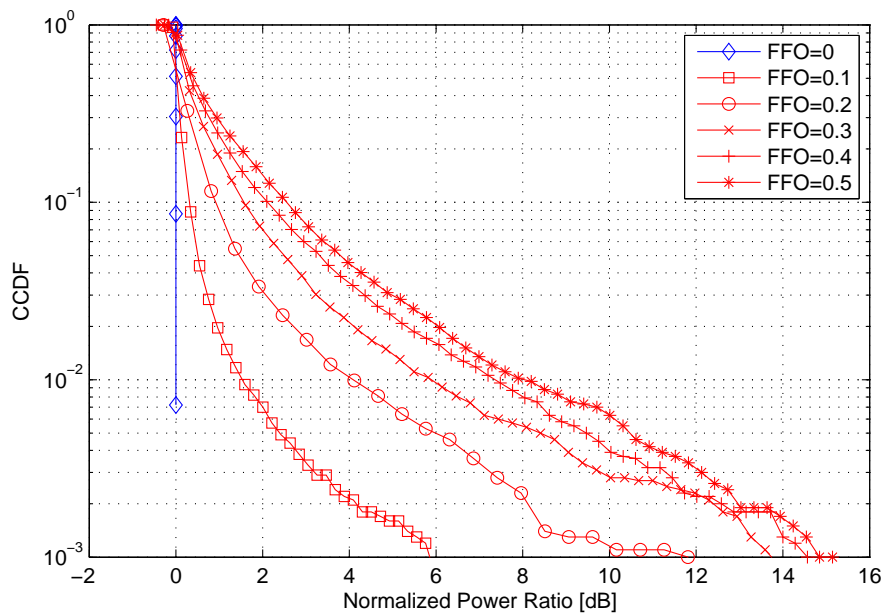
Figure 2.6: Power distribution normalized to zero-offset average power at different pre-compensated FFO values.
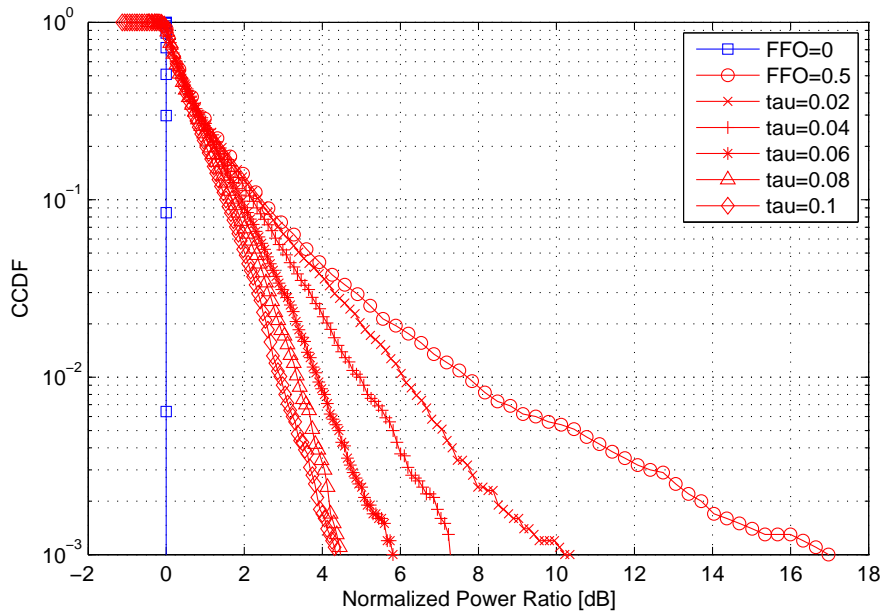
Figure 2.7: Power reduction for 0.5 FFO at different threshold values.

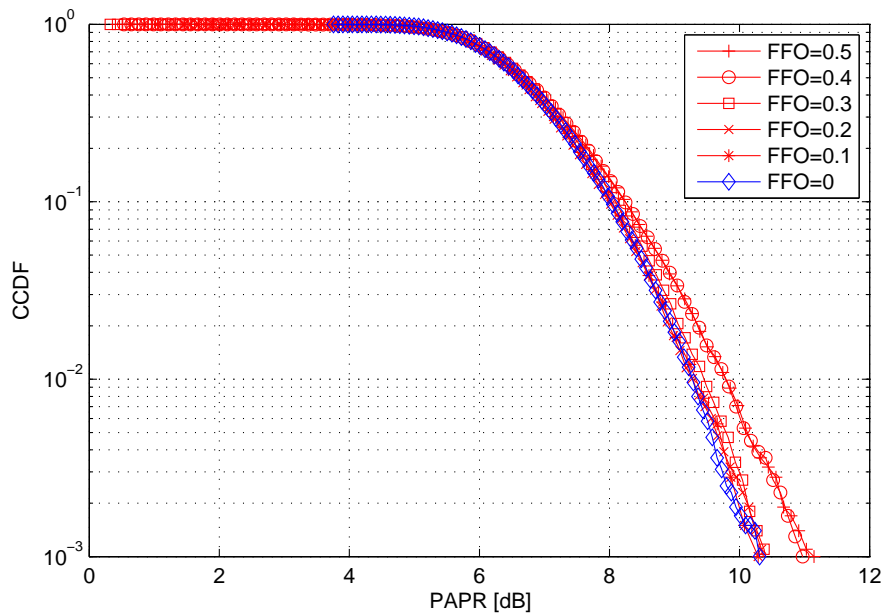factor affecting signal linearity and front-end design. Figures 2.5 and 2.6 show the distributions of the PAPR and the average power of the transmitted signal, for different offset values. While higher powers become more probable with increasing the offset value, this technique does not change PAPR much as shown.

A major contributor to the power increase is the inverse channel response $\mathbf{H_f^{-1}}$ in the pre-compensation stage. In a practical system, a threshold τ can be introduced as a design parameter. For subcarriers with estimated frequency response of magnitude $|H(k)| < \tau$, magnitude of the corresponding coefficients used in the pre-compensation stage are forced to this threshold value. This will reduce the power increase at the transmitter at the expense of a residual interference at the receiver. Moreover, it will create an error floor that depends on the value of the threshold. The same effect is introduced by channel estimation errors or imperfect channel reciprocity case. Shown in Fig.2.7 is the effect of different threshold values on the signal power in case of a 0.5 offset. While the PAPR is not affected by the threshold, transmitted power decreases as expected. Fig.3.1 shows the respective increase of the error floor. Hence, depending on the SNR range of operation, the threshold value is chosen to provide

17
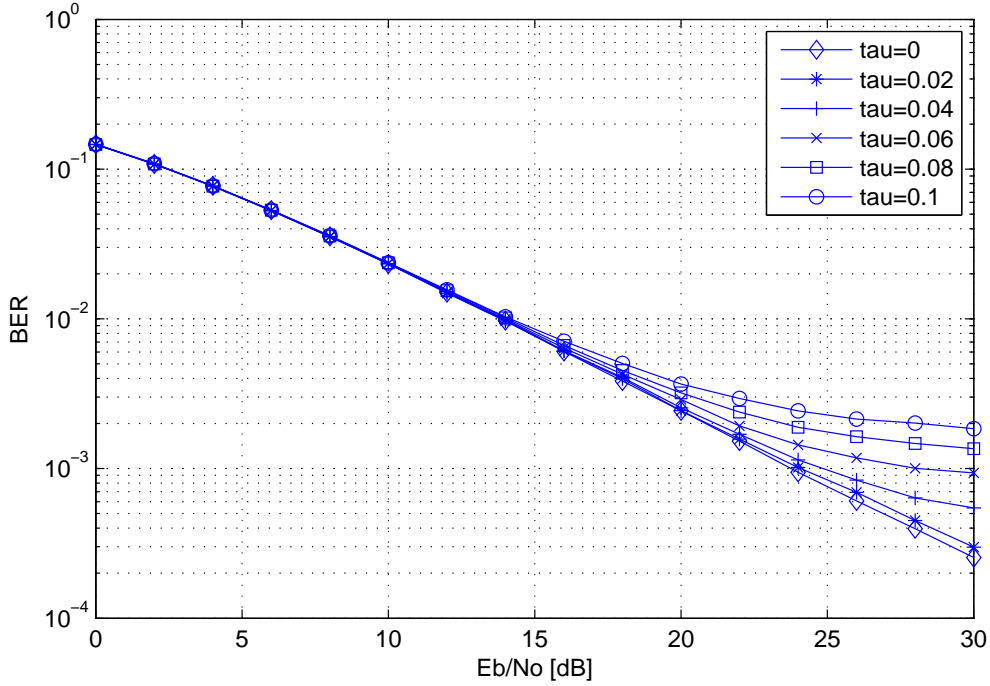
Figure 2.8: BER performance for 0.5 FFO at different threshold values.

an acceptable BER performance.

2.6 Conclusion

In this chapter, one of the critical drawbacks of OFDM systems is exploited for secrecy. The inter-carrier interference caused by carrier frequency offset is controlled to degrade the eavesdropper performance without affecting the performance of the legitimate user. This is feasible via the knowledge of the channel state information and the carrier offset value of the legitimate user. The simple structure of the proposed scheme shifts all the computational complexity from the mobile receiver to the base station, which makes it convenient for future low-consumption green radios. Also the power consumption of the scheme is treated. The choice of a threshold parameter provides acceptable performance depending on the SNR range of operation at the receiver.

Chapter 3

Enhancing Security in OFDM Systems Using Signal Space Diversity

3.1 Introduction

Diversity, originally used to mitigate the performance degradation on fading channels and increase transmission reliability, is also used to improve the security of wireless transmission [7]. Several types of diversities are used in the literature such as space diversity, cooperative diversity or frequency diversity. One of the most common techniques is to spread the signal in frequency via frequency hopping or spread spectrum (DS/SS) approaches [21]. This holds under the assumption of the eavesdropper not having any information regarding the spreading sequence. In [22], transmission is avoided on the faded subchannels of the frequency selective channel and artificial noise (AN) is inserted instead to further disturb the eavesdropper. Transmitter beamforming is proposed in [23] to facilitate the transmission confidentiality. Transmit antenna selection is used in [24] to improve the security of MIMO systems. Practical space-time coding is used in [25] and, with the collaboration of legitimate users in a

cluster, a space-time network coding scheme is proposed to prevent eavesdropping in [26]. Cooperative relays are used in [27] for improving security. Also time diversity provided by automatic repeat request (ARQ) is used in [28] to increase the security gap in terms of packet error rate.

Another type of diversity which has not received that much attention is signal space diversity. Most diversity techniques aim to provide statistically independent copies of the transmitted sequence at the receiver for reliable detection. While they usually require extra resources or power consumption, SSD provides performance improvement over fading channels by taking advantage of the inherent orthogonality in the signal space [8, 9]. The basic idea of SSD is to transmit the quadrature components of each multidimensional signal constellation point over independent fading channels. By simply interleaving these components prior to transmission, the independence of the fading channels can easily be accomplished [29].

Many of the security approaches in the literature rely on the rich multipath environment, which provides enough uncorrelation between the spatially separated wireless channels of the legitimate user and the eavesdropper. To avoid the leakage of the unique CSI of the user to the eavesdropper, TDD systems are used where the channel reciprocity assumption can be exploited. However, many of these studies make ideal assumptions on the CSI at the Alice, Bob, or Eve, and ignore the practical imperfections that affect the achievable secrecy performance. Frequency division duplex (FDD) is a more challenging scenario for security in terms of the CSI leakage problem [6]. In this chapter we propose a security technique that uses the conventional scheme of performing CSI feedback and thus can be viewed as a worst-case scenario technique in terms of security, where CSI of both the main and the wiretap channels are available at Eve.

Another advantage of our scheme is that it does not need multiple requirements such as, additional transmitted power for AN, information of the eavesdropping channel and location, multiple Tx and Rx antennas or cooperating nodes. With limited computational complexity for detection, we are able to improve the error performance

at Bob compared to Eve. By adapting the interleaving pattern of SSD to the channel of Bob, more diversity gain is delivered to Bob than Eve, since they experience independent fading. This relative gain in channel conditions allows us to improve the secrecy performance of the system.

This chapter is organized as follows: SSD system model is briefly explained in Section 3.2, followed by our proposed adaptation for OFDM security enhancement in Section 3.3. Section 3.4 presents the performance evaluation while conclusions are drawn in Section 3.5.

3.2   System Model

In phase shift keying (PSK) or quadrature amplitude modulation (QAM) constellations, the in-phase (I) and the quadrature (Q) channels are orthogonal and can be separated at the receiver. Therefore, transmitting these two components through independently fading channels introduces a diversity gain into the system. This can be achieved by independently interleaving the I and Q channels. However, this diversity gain is useful only if there is a redundancy between the two quadrature components. This is where the rotation angle of the constellation plays an important role [30]. Fig.3.1 shows a block diagram of an OFDM system employing SSD. Originally, the concept of coordinate interleaving and constellation rotation was used for frequency non-selective slowly fading channel where interleaving can be performed over time. In our work, we take advantage of the OFDM system performance in frequency selective channels. Hence, interleaving can be performed to subcarriers over each OFDM symbol, making the added delay independent of the interleaver depth. This allows us to make use of the uncorrelation of the spatially separated wireless channels for the sake of security.

The concept of SSD is generic to all PSK/QAM constellations, hence we confine our analysis to PSK signal constellations for simplicity. Introducing the redundancy needed for diversity can be achieved by rotating the signal constellations by a certain
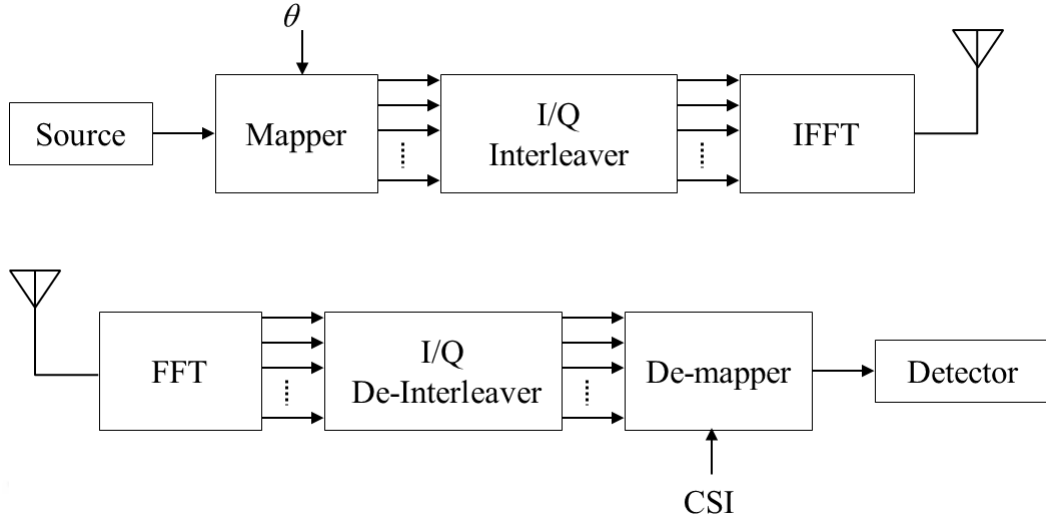
Figure 3.1: OFDM system model employing SSD.

angle θ. The modified MPSK constellation can be written as

$$S_M = \{s_p = e^{j(2\pi p/M + \theta)} : p = 0, 1, ..., M-1\} \tag{3.1}$$

where each symbol corresponds to $\log_2 M$ bits. The choice of the optimal rotation phase depends on the fading channel. In [9], the rotation angles are calculated at high SNR to maximize the minimum product distance of the rotated constellations over Rayleigh fading channels. In [29], the average BER is approximated by considering only the nearest neighbors and the rotation angles are also chosen based on this approximation. The exact pair-wise error probability for Rayleigh fading channels is calculated in [30] where rotation angles are optimized by minimizing the upper bound on the average BER.

Each quadrature component is then independently interleaved. The interleaving in our scheme is done in the frequency domain over each OFDM symbol. For N number of subcarriers, let the sequence of rotated I and Q components be denoted as $x = (x_0, x_1, ..., x_{N-1})$ and $y = (y_0, y_1, ..., y_{N-1})$, respectively. Let z_I and z_Q represent the I and Q interleavers, resulting in sequences $\bar{x} = z_I(x)$ and $\bar{y} = z_Q(y)$ which are to be transmitted over the N subcarriers.

The communication channel is assumed to be frequency selective fading channel.

Let the discrete channel frequency response of the OFDM system be denoted as $H = (H_0, H_1, ..., H_{N-1})$ where $H_k = |H_k|e^{j\phi_k}$ is the complex coefficient of the kth subcarrier. These coefficients are generated from the channel time impulse response where the taps are modeled as i.i.d. zero-mean complex Gaussian random variables in a Rayleigh fading channel. For the OFDM system and assuming perfect synchronization at the receiver, the received symbols after FFT can be written as

$$r = H\bar{s} + n \tag{3.2}$$

where $\bar{s} = \bar{x} + j\bar{y}$ is the vector of the transmitted interleaved symbols and n is a complex vector of additive white Gaussian noise with zero mean and a variance of $N_0/2$ in each dimension. Since the CSI is available at the receiver via channel estimation, the phase shift of the channel response $e^{j\phi_k}$ can be removed without any error. The received I and Q components are then de-interleaved to give $\bar{r}_I = z_I^{-1}(r_I)$ and $\bar{r}_Q = z_I^{-1}(r_Q)$. The magnitude of CSI is also de-interleaved resulting in $|H_I| = z_I^{-1}(|H|)$ and $|H_Q| = z_Q^{-1}(|H|)$. The receiver can then perform a maximum likelihood detection on the de-interleaved sequence

$$\bar{r} = |H_I|x + j|H_Q|y + \bar{n} \tag{3.3}$$

where $\bar{r} = \bar{r}_I + j\bar{r}_Q$ and $\bar{n}$ are the received signal and noise respectively after de-interleaving.

3.3 Enhancing Communication Security via SSD

The proposed eavesdropping-resilient OFDM system with SSD depends on delivering more diversity gain to Bob compared to Eve. It is shown in previous studies that the gain of SSD depends on the Euclidean distance between constellation points which is a function of the rotation angle under independent fading of I and Q components [30]. For a certain rotation angle, larger difference in the fading components provides larger gain. This can be understood as when one component goes through deep fading, the other component should provide enough separation distance in the signal space to offer more protection against noise, so that no two constellation points collapse together along any of the quadrature components [8].
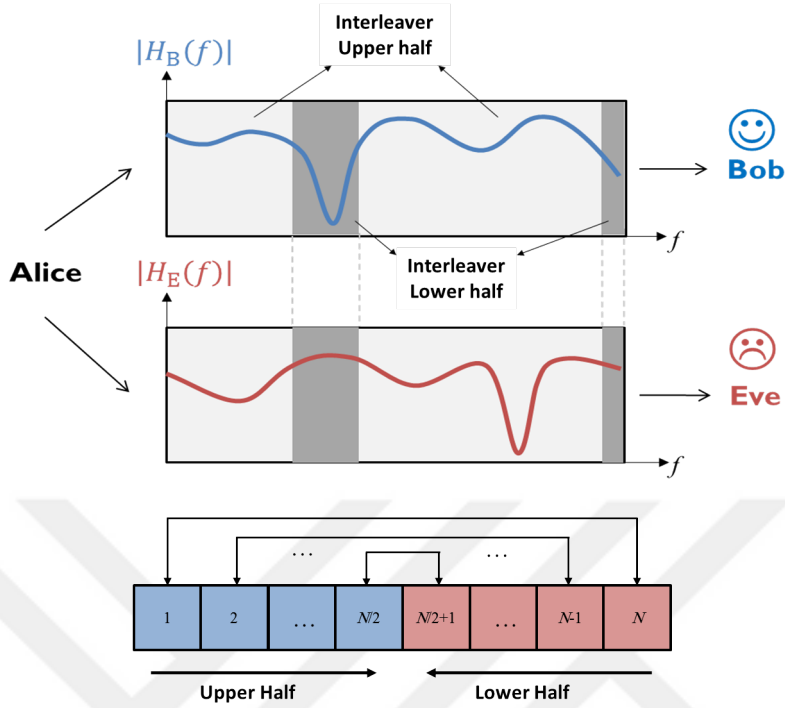
Figure 3.2: Adapting interleaving pattern to the channel response to provide more diversity gain to Bob than Eve.

3.3.1 Interleaving Pattern Adaptation

In order to provide more gain to Bob, we adapt the interleaving pattern to his CSI such that components going through bad channel condition, i.e. deep fades, are interleaved with ones going through good channel condition. This is done by first sorting the channel coefficients H according to the descending order of their magnitudes. The order of the N subcarriers can be expressed as

$$|H_k(1)| \geq |H_k(2)| \geq \ ... \geq |H_k(l)| \geq ... \geq |H_k(N)| \tag{3.4}$$

where k is the exact position of the subcarrier and l denotes the subcarrier order index among the N sorted subcarriers. Then the interleaving pattern is designed so that the upper half of the sorted magnitudes should replace the lower half by moving from the ends to the middle as shown in Fig.3.2. This way, we make sure that each bad component is interleaved with the best component possible. The interleaved

pairs would have the l indices of

$$\{ \ (1, N), \ (2, (N-1)), \ ... \ (N/2, (N/2+1)) \ \} \tag{3.5}$$

As mentioned before, our scheme makes use of the channel spatial dependency, meaning that wireless channels associated with different end points at separate locations typically exhibit uncorrelated propagation characteristics in rich scattering environments. As a result, the eavesdropping channel H^E would be uncorrelated with the main channel H. The de-interleaved signal at Eve can be written as

$$\bar{r}_E = |H_I^E|x + j|H_Q^E|y + \bar{n}_E \tag{3.6}$$

3.3.2 Eavesdropper Gain Reduction

Since this is a CSI-based security scheme, the time variation of the wireless channels introduces frequently updated randomness, which further strengthens its security. In FDD systems, the CSI is fed back to the transmitter so that it can adapt its transmission parameters accordingly. In some scenarios, the CSI may be outdated due to insufficient feedback bandwidth, causing the main channel at Alice to consist of only the past channels. Since the channel is slowly fading, using the past channel for the interleaving pattern design will not have a large effect on the diversity gain delivered. Hence, Bob can also use the past channel for interleaving adaptation while the current channel is used for normal detection. Since the CSI is fed back from Bob to Alice, Eve can intercept the transmission to acquire the interleaving pattern and use it for detection. However, even if she manages to use the same de-interleaver as Bob, the gain delivered is not the same due to the uncorrelation between their channels, as shown in Fig.3.2. In fact, the performance of Eve will be the same as SSD with random interleaving, as we will show later on.

However, if we take a closer look at the interleaved pairs in (3.5), we notice that not all the pairs contribute identically to the diversity gain. In fact, most of the gain comes from the first portion of pairs, and as we move forward, the contribution becomes less significant. This comes from the fact that, the interleaved channel

magnitude pairs at the end are close to each other in order, hence they have the minimum differences among subcarriers. We can take advantage of this by reducing the interleaver depth to include just the contributing pairs and keep the remaining subcarriers without interleaving. In addition to reducing computational complexity, this has the advantage of significantly reducing the gain delivered to Eve. Since the chosen interleaved pairs are optimum for Bob's channel, more gain reduction is delivered to Eve compared to Bob.

3.4   Performance Evaluation

3.4.1   Performance Analysis over Fading Channels

Considering a QPSK scheme for our analysis, the conditional average bit-error probability can be written as

$$P(s_p \rightarrow \hat{s}_p | \alpha) = Q\left(\sqrt{\alpha d_{min}^2}\right) \tag{3.7}$$

where $\alpha = |H|^2 \dfrac{E_b}{N_0}$ is the faded SNR per bit and d_{min}^2 represents the minimum squared Euclidean distance between two constellation points. It can also be represented as the sum of the distances in the I and Q directions $d_{min}^2 = d_I^2 + d_Q^2$ where

$$d_I^2 = 1 + \sin(2\theta)$$
$$d_Q^2 = 1 - \sin(2\theta) \tag{3.8}$$

In this work, the fading amplitude is modeled as Rayleigh fading with unity average power. Hence α has the PDF and CDF of

$$f_\alpha = \frac{1}{\bar{\alpha}} e^{-\alpha/\bar{\alpha}} \tag{3.9}$$

$$F_\alpha = 1 - e^{-\alpha/\bar{\alpha}} \tag{3.10}$$

26

respectively, where $\bar{\alpha} = \dfrac{E_b}{N_0}$ is the average SNR per bit and, in (3.7), $Q(x)$ is the Gaussian probability function defined as

$$Q(x) = \frac{1}{\pi} \int_0^{\frac{\pi}{2}} e^{\frac{-x^2}{2\sin^2\phi}} d\phi. \tag{3.11}$$

For the proposed adaptive interleaver, the two fading components α_1 and α_2 can not be considered exponentially distributed as in (3.9) anymore. Since our algorithm sorts the subcarriers according to the fading magnitude, the distribution of the fading components over each subcarrier follows an order statistic that depends on the subcarrier order index l and the total number of subcarriers N.

For a sequence of i.i.d. random variables $\{\alpha_1, \alpha_2, ..., \alpha_N\}$ of length N, PDF f_α and CDF F_α, the PDF of the kth order statistic, that is, the k smallest of the sequence, is given by [31]

$$f_k = \frac{N!}{(k-1)!(N-k)!} F_\alpha^{k-1} [1 - F_\alpha]^{N-k} f_\alpha. \tag{3.12}$$

Hence, for a subcarrier with the interleaved pair of order indeces (k_1, k_2), the distribution of the fading components α_1 and α_2 follows the order statistics f_{k_1} and f_{k_2} from (3.12) respectively, and the bit-error probability can be calculated as

$$P_s(k_1, k_2) = \int_0^\infty \int_0^\infty Q\left(\sqrt{\alpha_1 d_I^2 + \alpha_2 d_Q^2}\right) f_{k_1} f_{k_2} d\alpha_1 d\alpha_2 \tag{3.13}$$

$$= \sum_{u_1=0}^{k_1-1} \sum_{u_2=0}^{k_2-1} A \binom{k_1 - 1}{u_1} \binom{k_2 - 1}{u_2} (-1)^{u_1+u_2}$$

$$\left[1 - \frac{\beta}{\beta - \gamma} \sqrt{\frac{\beta}{1+\beta}} + \frac{\gamma}{\beta - \gamma} \sqrt{\frac{\gamma}{1+\gamma}} \right], \tag{3.14}$$

where

$$A = \frac{\dfrac{N!}{2(k_1 - 1)!(N - k_1)!(u_1 + N - k_1 + 1)}}{\dfrac{N!}{(k_2 - 1)!(N - k2)!(u_2 + N - k_2 + 1)}},$$

$$\beta = \frac{d_I^2 \bar{\alpha}}{2(u_1 + N - k_1 + 1)},$$

$$\gamma = \frac{d_Q^2 \bar{\alpha}}{2(u_2 + N - k_2 + 1)}.$$

27

The exact derivation of (3.14) can be found in the appendix. According to (3.5), for a total number of N subcarriers, the orders take the values $k_1 \in \{1, 2, .., N\}$ while $k_2 = N + 1 - k_1$. As a result, (3.13) can be written as a function of only k_1 and the total average bit-error probability is calculated by averaging over the N subcarriers

$$P_e = \frac{1}{N} \sum_{k_1=1}^{N} P_s(k_1). \tag{3.15}$$

3.4.2 Simulation Results

The security of the proposed OFDM system employing SSD is evaluated through the BER of Bob and Eve over fading channels. We take QPSK as the candidate constellation in MPSK signal constellations and present the simulation results over Rayleigh fading multipath channels with uniform power delay profile. We assume identical statistical models for both the main channel and the wiretap channel. In order to make fair comparisons, we also assume that the noise levels at all nodes are the same. First we show the simulation results for the optimum rotation angle for QPSK signal constellations. Fig.3.3 shows the BER performance at $E_b/N_0 = 15$ dB with different rotation angles and random interleaving. The optimum rotation angle of 27.5^o matches the one calculated in [30] for natural bit mapping. Fig.3.4 shows the performance gain achieved by the SSD over the conventional modulation system for the optimum rotation angle calculated and $N = 64$ subcarriers. This gain is achieved using a certain random interleaver at both Alice and Bob. It is also shown in the figure that, this is the same gain that can be delivered to Eve under the assumption that Eve can acquire the interleaver pattern used by Alice and Bob in FDD case. We also include the TDD case where the interleaving pattern does not match with Bob, since CSI is not known to Eve. It shows that the performance of Eve is totally degraded and secrecy is ensured. In addition, the figure shows that the gain delivered to Bob is larger than the normal SSD gain since we adapt the interleaver pattern to the main channel response.

As we mentioned before, the interleaver depth can be reduced without losing much of the performance gain for Bob. Fig.3.5 shows the performance for different values
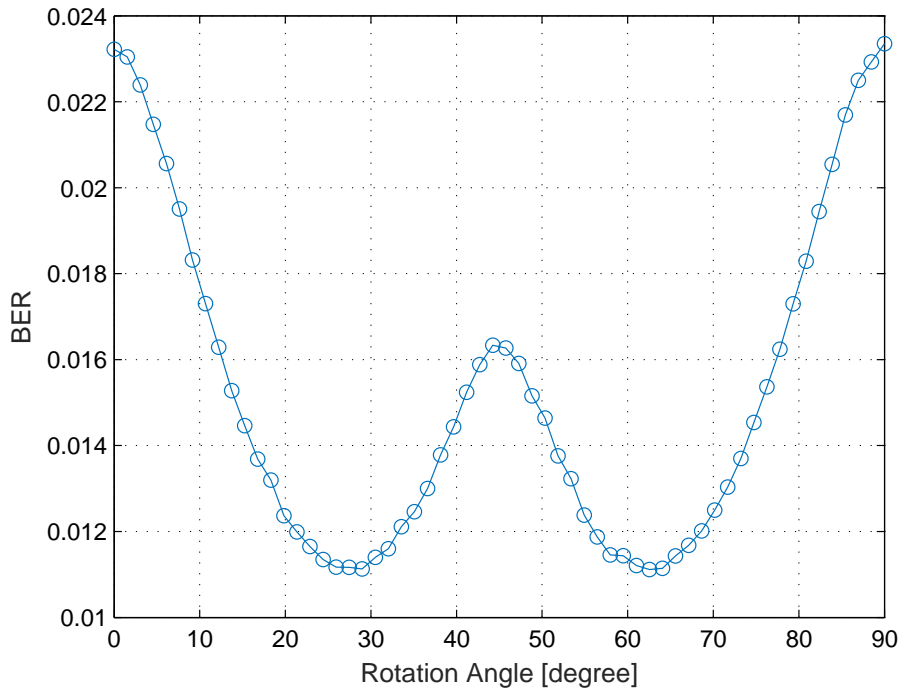
Figure 3.3: Average BER of QPSK signal constellation at different values of the rotation angle θ over Rayleigh channel at $E_b/N_0 = 15$ dB.

of interleaving depth as percentage of the N subcarriers at SNR = 20 dB. Keeping in mind that it is in log scale, we see that the gain reduction for Eve is very large compared to Bob. Based on the acceptable performance of Bob, the interleaver depth can be chosen to minimize the gain delivered to Eve. Fig.3.6 shows the performance gain for Bob and Eve for interleaver depth of 50%. It is clear that the diversity gain delivered to Eve over the conventional system is becoming insignificant compared to Bob.
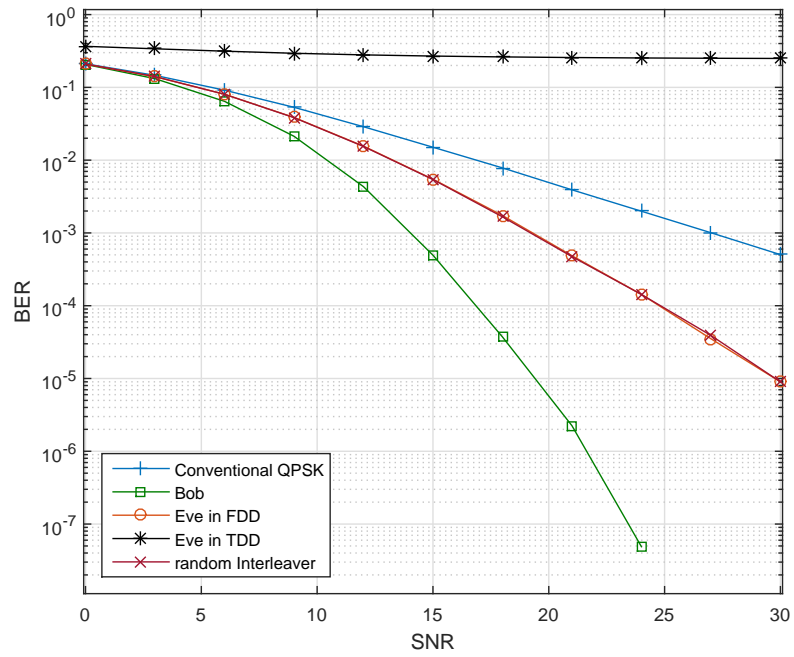
Figure 3.4: Average BER of QPSK signal constellation at different SNR over Rayleigh channel at $\theta = 27.5^o$.
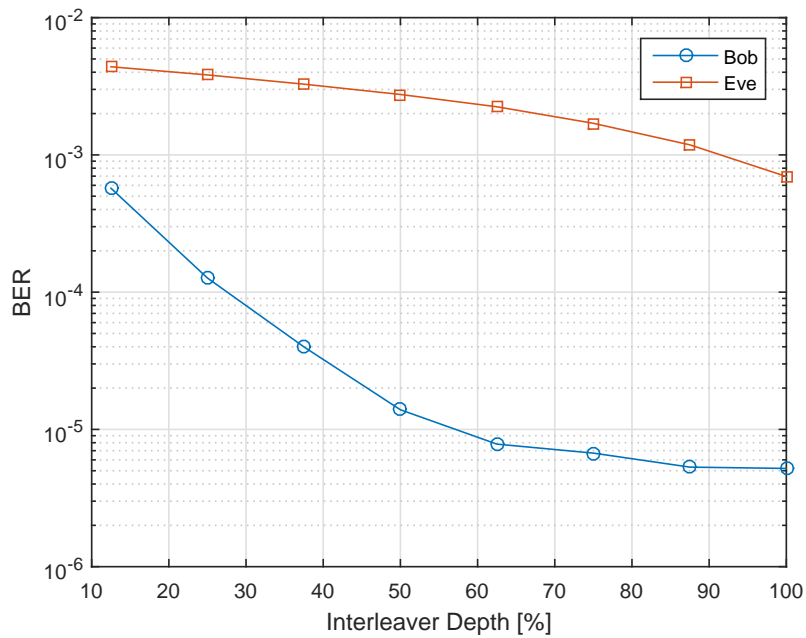
Figure 3.5: Average BER of QPSK signal constellation at different percentage values of the interleaver depth over Rayleigh channel at SNR = 20 dB.
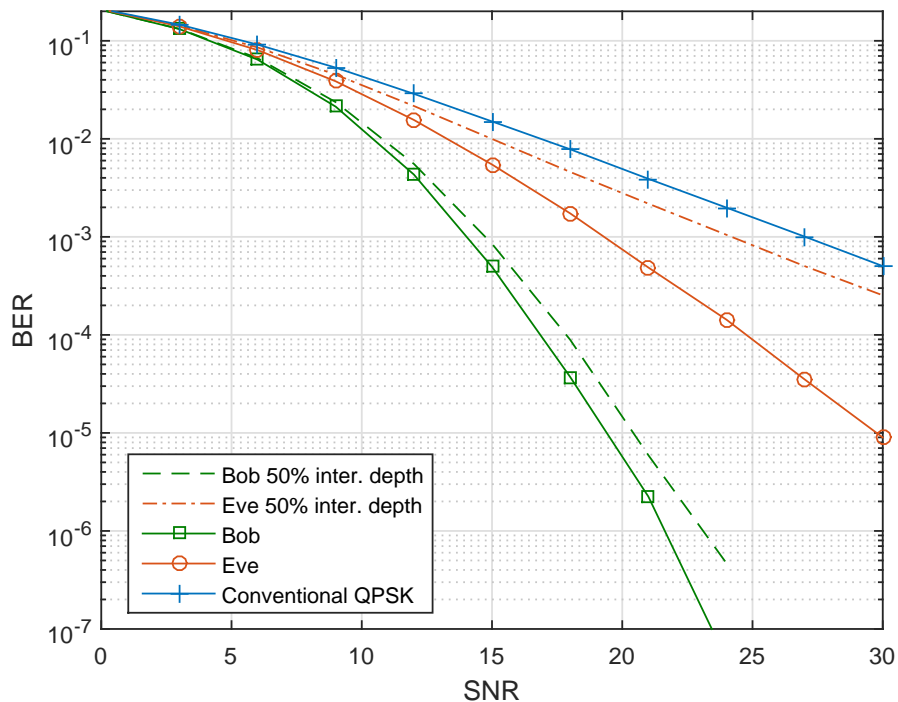
Figure 3.6: Performance reduction in average BER at different SNR with 50% interleaver depth.

3.5 Conclusion

The randomness of the wireless multipath channel is used to provide more diversity gain to the legitimate user compared to an eavesdropper. Using signal space diversity, we are able to enhance the error performance by adapting the interleaving pattern to the unique channel response of the legitimate user. This scheme is robust against the channel state information leakage problem usually faced in wireless communication, hence conventional FDD systems can make use of this scheme. The design of an optimal interleaver is presented with a trade off between computational complexity and error performance.

Chapter 4

Location-specific Secure Transmission Using CoMP Directional Modulation

4.1 Introduction

Many of the techniques found in literature rely on the the rich scattering environment which provides enough uncorrelation between the multipath channels of legitimate users and eavesdroppers. This allows the user to have a unique CSI that can be used for securing the transmission in case the transmitter has this knowledge. Hence for open environments, where scatterers are limited or LOS dominates the communication, other techniques are needed. This problem has been conventionally addressed using multiple antenna techniques. Smart antennas include a broad variety of technologies ranging from switched beam antennas to more sophisticated adaptive arrays [32]. With appropriately chosen weights, antenna arrays can be used to focus the communication energy spatially, hence maximizing the signal quality at user direction and place nulls in other directions. This beamforming property has allowed smart antennas to be used for physical layer security.

Directional Modulation is a multiple antenna technique that was recently developed for secure transmission [10, 11]. Unlike the conventional beamforming where same information is transmitted to all directions, DM transmits the desired data in the direction of legitimate user and randomize the field pattern in all other directions. Hence, improving sensitivity of a receiver or reducing the distance between transmitter and receiver are not helpful for decoding information outside information beams. This directional security is done by moving the modulation step to RF front-end stage where direction selectivity is controlled by antenna arrays.

The work in [33] introduced the multiple directions DM transmission scheme (MDDM). They were able to provide multiple secure communication links for different directions. They showed that the scheme increases the transmission capacity of the system up to the number of the antenna elements. Also, the secrecy capacity increases with the increase of the number of transmitted streams. Moreover, MDDM has a low complexity structure compared to other DM implementations and it does not necessitate the implementation of special receiver algorithms.

An obvious drawback of this scheme is that any receiver along the information beam can easily intercept the signal. To overcome this scenario, a coordinated multipoint transmission scheme is proposed in this chapter. Using multiple geographically separated base-stations (BS) to transmit the signal allows the data to be decodable only at the intersection of their information beams while being distorted at other locations. In other words, a receiver along the information beam of any BS is under interference from the other BSs except at users locations where all signals add up to give the desired data. While we put extra load on the back-haul network for coordination, it is only limited to data sharing. Since the assumption of the channel knowledge is relaxed, computational complexity is reduced for both users and base stations. In this context, we define a metric called Clear Region that refers to the area within which a receiver can access and decode the signal being transmitted to a legitimate user.

The rest of the chapter is organized as follows: in Section 4.2, we introduce the construction of DM algorithm followed by our proposed CoMP scheme. The Clear Region metric is defined in Section 4.3. Finally, Section 4.4 presents performance evaluation and the effect of number of antennas and modulation order on CR, while conclusions are given in Section 4.5.

4.2 System Model

4.2.1 Directional Modulation

We consider a broadcast channel with a single BS and L users each at different direction. The base station uses a linear antenna array with N elements for transmission where $N \geq L$. Each direction has its own desired data stream and transmission angle with respect to the base station. Assuming isotropic antenna elements d distance apart, the resultant field pattern at time instant n and direction angle θ is given by [33]

$$f(\theta, n) = h(\theta)W(n) \tag{4.1}$$

$$h(\theta) = [e^{-j(\frac{N-1}{2})\frac{2\pi d}{\lambda}cos\theta}, e^{-j(\frac{N-1}{2}-1)\frac{2\pi d}{\lambda}cos\theta}, .. \tag{4.2}$$
$$e^{j(\frac{N-1}{2})\frac{2\pi d}{\lambda}cos\theta}]$$

where $W(n) = [w_1(n), w_2(n), ..., w_N(n)]^T$ is the vector containing the complex weights for the antenna array and $h(\theta)$ is the array steering vector for a receiver at direction θ. Based on the concept of DM, we need to set the complex weights for the antenna array W, so that the field pattern complex value equals to the transmitted symbol at the desired angle of each user direction. This is done by solving an underdetermined set of linear equations using the least-norm solution as shown in [33] which gives

$$W(n) = H^H(HH^H)^{-1}X(n) \tag{4.3}$$

where $H = [h(\theta_1)h(\theta_2)..h(\theta_L)]^T$ is a complex matrix of size $(N \times L)$ and $X(n) = [x_1(n), x_2(n), ..., x_N(n)]^T$ is the complex vector of the symbols to be transmitted to
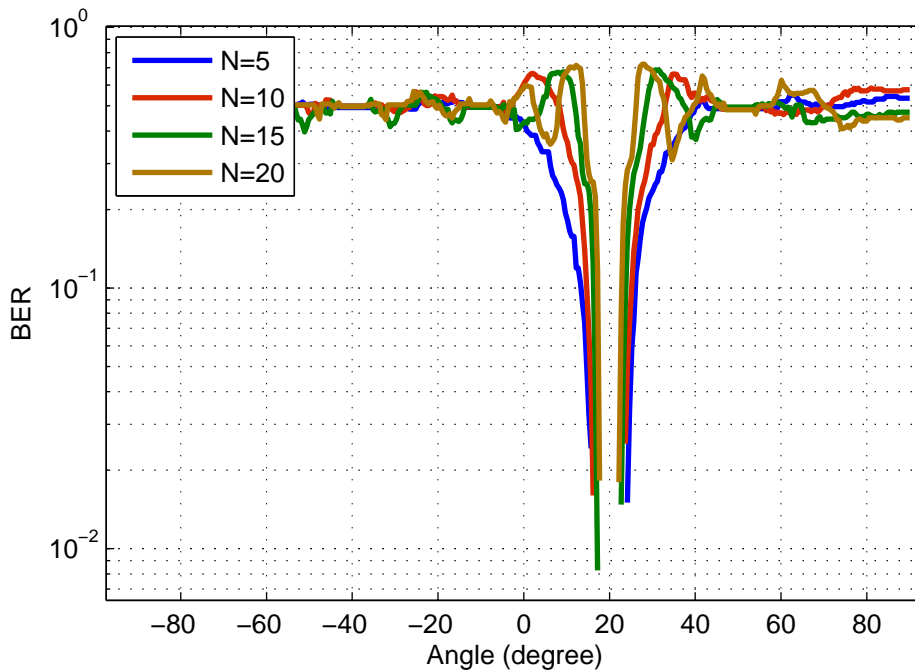
Figure 4.1: BER performance at different angles with a user at $\theta = 20°$ using 16-QAM and different antenna array sizes.

each direction. The performance can be further enhanced using CSI of the legitimate users if available at the transmitter as suggested in [33]. They also show how the information beamwidth decreases as we increase the order of modulation used. Another way of controlling the beam width is to switch the number of antenna array elements. Fig.4.1 shows the noiseless BER performance of a single base station with a user at 20° direction for different antenna array sizes using 16-QAM modulation. While we managed to hide the signal in all the other directions, still the signal in the direction of the intended user is not secured.

4.2.2 Coordinated Multipoint Transmission

CoMP refers to a wide range of techniques that enable dynamic coordination or transmission with multiple geographically separated base stations to enhance the end user service quality even at cell edges [34]. One of the major categories for CoMP

downlink transmission is the joint processing and transmission scheme where data is transmitted simultaneously from all base stations to improve the received signal quality and strength or to cancel interference from other users. To that end, highly detailed feedback is required on the channel properties in a fast manner. Another requirement is for a very close coordination between the base stations to facilitate the combination of data or fast switching of the cells.

For our proposed approach, we do not need to know the CSI of the users, only the location information is required, that is, the angle of each user from each BS. Also the strict timing coordination can be relaxed since we are sending the same data from all base stations, hence the delayed signals can be accounted as multi-path components. The signal received at any location $r(t)$ will be the combination of the simultaneous transmission from each base station $s_i(t)$ plus the additive Gaussian noise $z(t)$ at the receiver,

$$r(t) = \sum_{i=1}^{B} g_i(t - \tau_i)s_i(t) + z(t). \tag{4.4}$$

where B is the number of BSs, g_i is the channel gain coefficient associated with the transmission of the ith BS, and τ_i is the corresponding delay. The transmitted signals directed to the location of a legitimate user from all BSs will be the same as

$$s_i(t) = s_{Conf}(t) \quad \forall i \tag{4.5}$$

where $s_{Conf}(t)$ is the confidential message intended for the legitimate user. On the other hand, at any other location the B signals will not be the same due to the directional modulation selectivity which inherently causes interference to all directions outside the information beams.

Another approach would be using the CSI at the transmitter to further improve the secrecy performance as shown in previous sections. That would allow the base stations to divide the data into different components each transmitted from a base station. Since the channel effect would already be pre-compensated, the data can be divided in such a way that the signals can be coherently added at the users locations to give the intended data. This division pattern is not needed to be known at the receiver, hence it can be changed continuously to further secure the transmission.

4.3 Clear Region Calculation

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

$$CR = \frac{1}{M} \sum_{i=1}^{M} CR_i \tag{4.6}$$

where the clear region of the ith user CR_i is the region in which a receiver can decode the data of the ith user.

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

$$CR_i = \frac{1}{K} \sum_{k=1}^{K} U\left(\eta - BER_k\right) \tag{4.7}$$

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

4.4 Simulation Results

The CoMP scheme requires the signal to be transmitted from several geographically separated base stations to provide a means of security so that, along each direction of transmission, the data is not decodable. Here, we simulate a 100×100 area ($K = 10^4$)

covered by 3 BSs ($B = 3$). The number of users served in that area is based on the number of used antenna elements ($M = N = 8$). The secrecy threshold is chosen as $\eta = 10^{-2}$. Fig.4.2 shows the simulation of the equally separated base stations. The BSs are configured such that the broadside direction of each antenna array is pointing towards the center of the equilateral triangular shape of the base stations positions. Using antenna arrays size of 8 and 4-QAM modulation scheme, contours of the noiseless BER performance for one of the users is shown where circles represent the users and squares are the BSs. Fig.4.3 shows the case where 16-QAM modulation is used. Notice how the secure region area is reduced with increasing the modulation order. To further control the secure area, the number of activated antenna arrays elements is changed accordingly. Increasing the number of antenna elements narrows the information beam-width, reducing the CR area as shown next.

In order to profile the performance of this security technique, we use the average CR metric to measure how the secure location is being varied. Fig.4.4 shows the effect of varying the number of antenna elements of the base stations. It is clear that, for a given modulation order, as the number of elements increases, the CR is reduced significantly. Furthermore, different modulation orders are simulated. As mentioned previously, higher modulation order allows for more confined CR. Hence, using both: antenna size and modulation order, full control over the secure region is attained.
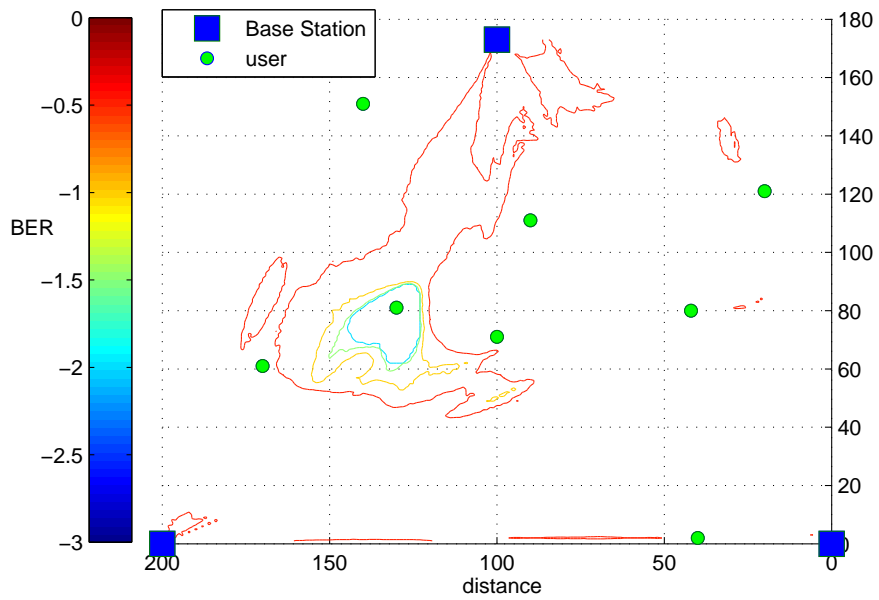
Figure 4.2: BER performance contour with 4-QAM and N=8.
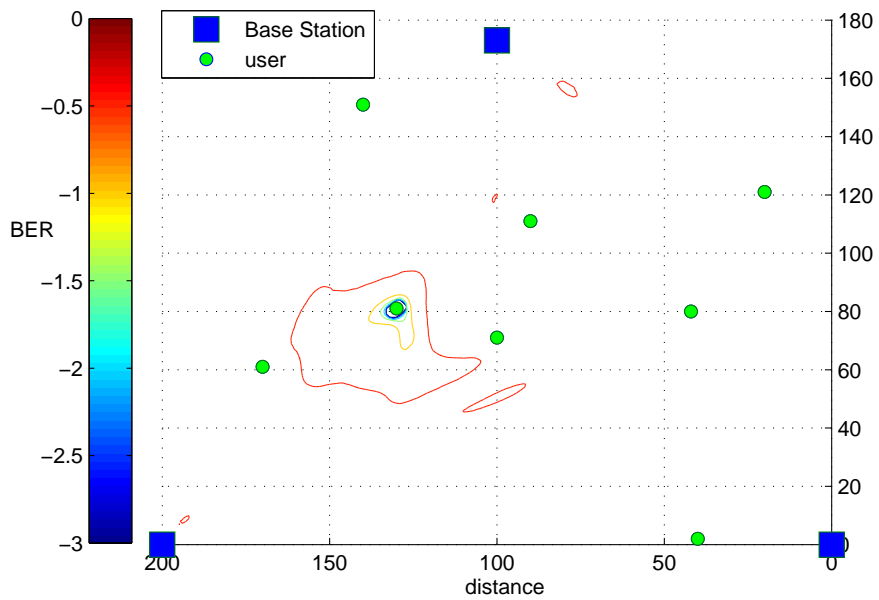
Figure 4.3: BER performance contour with 16-QAM and N=8.
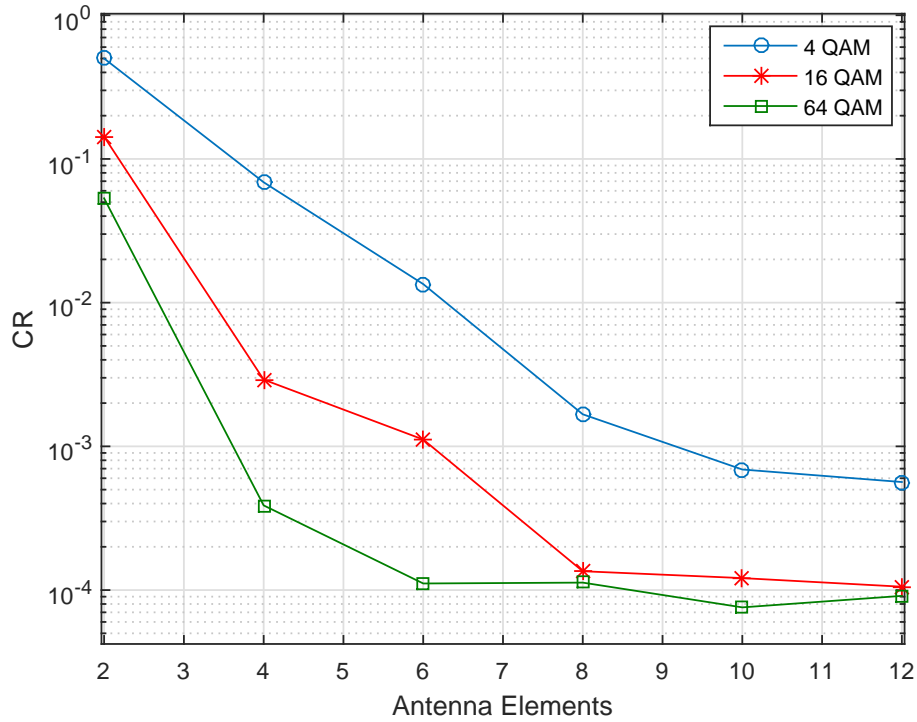
Figure 4.4: Clear region reduction with number of antenna elements for different modulation orders.

4.5 Conclusion

A novel location-specific multi-user secure scheme is proposed using coordinated multipoint transmission with directional modulation. The new technique exploits the information of users locations to create a clear region for users to decode the data. The desired region is covered by more that one base station and the clear region area is controlled by switching the number of antenna array elements or changing the transmission modulation order. Simulations validate the performance of this scheme for different antenna sizes and modulation orders using the proposed clear region metric.

Chapter 5

Concluding Remarks

Securing wireless communications is a challenging task. The broadcast nature of the wireless medium allows possible adversaries to eavesdrop on the information being transmitted. Alongside the conventional cryptography-based solutions, physical layer security provides a promising paradigm. Taking advantage of the propagation characteristics and randomness of the wireless channel, several techniques are developed to provide security and privacy to the transmitted message.

In this thesis, we propose a technique that makes use of the rich multipath environment in a time division duplex system. One of OFDM critical issues, carrier frequency synchronization, is exploited for the sake of security. By controlling the inter-carrier interference caused by a carrier offset between the legitimate receiver and transmitter, we introduce interference to the eavesdropper while pre-compensating the interference effect only for the legitimate user. Also we discuss a technique that can be adopted for frequency division duplex systems where the channel state information of the legitimate user is fed back to the transmitter on a separate channel. We use signal space diversity to provide more gain to the legitimate user by using the interleaver in frequency domain and adapting the interleaving pattern to his channel response, leaving the eavesdropper with insignificant diversity gain.

Finally, we complete our work with a security scheme that deals with open environments with limited scatterers. This line-of-sight type of transmission is often secured using multiple antenna techniques such as directional modulation. To make the signal meaningful only at the location of the legitimate users, directional modulation is proposed in a coordinated multi-point system with a newly defined metric for characterizing the performance of this scheme. As we elaborated, the proposed techniques can be used for independent scenarios or can be combined together to provide the highest level of security.

Bibliography

[1] A. D. Wyner, "The Wiretap Channel," Bell Syst. Tech. Journal, vol. 54, pp. 1355-1387, 1975.

[2] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian Wiretap Channel," IEEE Trans. Inform. Theory, vol. 24, no. 4, pp. 451-456, Jul. 1978.

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

[4] K. Ren, H. Su, and Q. Wang, "Secret Key Generation Exploiting Channel Characteristics in Wireless Communications," IEEE Wireless Commun., vol. 18, no. 4, pp. 6-12, Aug. 2011.

[5] T. Yucek and H. Arslan, "OFDM signal identification and transmission parameter estimation for cognitive radio applications," Proc. IEEE Global Telecomm. Conf. (Globecom), Washington, D.C., USA, Nov. 2007.

[6] T. Y. Liu, P. H. Lin, S. C. Lin, Y. W. P. Hong and E. A. Jorswieck, "To avoid or not to avoid CSI leakage in physical layer secret communication systems," in IEEE Commun. Mag., vol. 53, no. 12, pp. 19-25, Dec. 2015.

[7] Y. Zou, J. Zhu, X. Wang and V. C. M. Leung, "Improving physical-layer security in wireless communications using diversity techniques," in IEEE Network, vol. 29, no. 1, pp. 42-48, Jan.-Feb. 2015.

[8] J. Boutros and E. Viterbo, "Signal space diversity: a power and bandwidth-efficient technique for the Rayleigh fading channel," IEEE Trans. Information Theory, vol. 44, no. 4, pp. 1453-1467, July 1998.

[9] G. Taricco and E. Viterbo, "Performance of component interleaved signal sets for fading channels," IEEE Electronics Letters, vol. 32, no. 13, pp. 1170-1172, April 1996.

[10] Daly, Michael P., and Jennifer T. Bernhard. "Directional modulation technique for phased arrays." Antennas and Propagation, IEEE Transactions on 57, no. 9 (2009): 2633-2640.

[11] Daly, Michael P., Erica Lynn Daly, and Jennifer T. Bernhard. "Demonstration of directional modulation using a phased array." Antennas and Propagation, IEEE Transactions on 58, no. 5 (2010): 1545-1550.

[12] X. Wang, P. Ho, and Y. Wu, "Robust channel estimation and ISI cancellation for OFDM systems with suppressed features," IEEE J. Select. Areas Commun., vol. 23, no. 5, pp. 963-972, May 2005.

[13] Z. E. Ankarali, M. Karabacak and H. Arslan, "Cyclic Feature Concealing CP Selection for Physical Layer Security," IEEE Military Commun. Conf. (MILCOM), 2014.

[14] T. Yucek, and H. Arslan. "Feature suppression for physical-layer security in OFDM systems," IEEE Military Commun. Conf. (MILCOM), 2007.

[15] T. Pollet, M. Van Bladel, and M. Moeneclaey, "BER sensitivity of OFDM systems to carrier frequency offset and Weiner phase noise," IEEE Trans. Commun., vol. 43, pt. 1, pp. 191?193, Feb.-Apr. 1995.

[16] Schmidl, M. Timothy, and C. Cox. Donald "Robust frequency and timing synchronization for OFDM," IEEE Trans. Commun., vol. 45, no. 12, pp. 1613-1621, 1997.

[17] J.-J. van de Beek, P. O. Borjesson, M.-L. Boucheret, D. Landstrom, J. M. Arenas, P. Odling, C. Ostberg, M. Wahlqvist, and S. K. Wilson, "A time and frequency synchronization scheme for multiuser OFDM," IEEE J. Sel. Areas Commun., vol. 17, no. 11, pp. 1900-1914, Nov. 1999.

[18] Z. Cao, U. Tureli, Y.-D. Yao, and P. Honan, "Frequency synchronization for generalized OFDMA uplink," Proc. IEEE Global Telecomm. Conf. (Globecom), vol. 2, Nov. 2004, pp. 1071-1075.

[19] J. Choi, C. Lee, H. W. Jung, and Y. H. Lee, "Carrier frequency offset compensation for uplink of OFDM-FDMA systems," IEEE Commun. Lett., vol. 4, no. 12, pp. 414-416, Dec. 2000.

[20] Barros, Joao, and Miguel Rodrigues, "Secrecy capacity of wireless channels," IEEE Inter. Symp. Inform. Theory, pp. 356-360, 2006.

[21] Y. Hwang and H. C. Papadopoulos, "Physical-layer secrecy in AWGN via a class of chaotic DS/SS systems: analysis and design," IEEE Trans. Signal Processing, vol. 52, no. 9, pp. 2637-2649, Sept. 2004.

[22] E. Guvenkaya and H. Arslan, "Secure communication in frequency selective channels with fade-avoiding subchannel usage," IEEE Inter. Conf. on Commun. Workshops (ICC), pp. 813-818, 2014.

[23] H. Koorapaty, A. Hassan and S. Chen., "Secure information transmission for mobile radio," IEEE Commun. Lett., vol. 4, pp. 52-55, Feb. 2000.

[24] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," IEEE Signal Process. Lett., vol. 19, no. 6, pp. 372-375, Jun. 2012.

[25] J. M. Hamamreh, E. Guvenkaya, T. Baykas, and H. Arslan, "A Practical Physical-Layer Security Method for Precoded OSTBC-Based Systems," IEEE Wireless Commun. and Net. Conf. (WCNC), pp. 1651-1656, April 2016.

[26] Y. Zou, Y.-D. Yao, and B. Zheng, "Opportunistic distributed space-time coding for decode-and-forward cooperation systems," IEEE Trans. Signal Process., vol. 60, no. 4, pp. 1766-1781, Apr 2012.

[27] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," IEEE Trans. Signal Process., vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[28] J. M. Hamamreh, M. Yusuf, T. Baykas, and H. Arslan, "Cross MAC/PHY Layer Security Design Using ARQ with MRC and Adaptive Modulation," IEEE Wireless Commun. and Net. Conf. (WCNC), pp. 1632-1638, April 2016.

[29] S. B. Slimane, "An improved PSK scheme for fading channels," IEEE Trans. on Vehicular Tech., vol. 47, no. 2, pp. 703710, May 1998.

[30] N. F. Kiyani, J. H. Weber, A. G. Zajic and G. L. Stuber, "Performance Analysis of a System using Coordinate Interleaving and Constellation Rotation in Rayleigh Fading Channels," IEEE Vehic. Tech. Conf., pp. 1-5, 2008.

[31] H. A. David, "Order statistics," New York, John Wiley & Sons, 1981.

[32] Mietzner, R. Schober, L. Lampe, W. H. Gerstacker and P. A. Hoeher, "Multiple-antenna techniques for wireless communications-a comprehensive literature survey," in IEEE Commun. Surv. and Tut., vol. 11, no. 2, pp. 87-105, 2009.

[33] M. Hafez and H. Arslan, "On Directional Modulation: An Analysis of Transmission Scheme with Multiple Directions," IEEE Intern. Conf. on Commun. (ICC), London, UK, June 2015.

[34] Irmer, Ralf, et al. "Coordinated multipoint: Concepts, performance, and field trial results." Communications Magazine, IEEE 49, no. 2 (2011): 102-111.

[35] M. Yusuf and H. Arslan, "Controlled Inter-carrier Interference for Physical Layer Security in OFDM Systems," IEEE Vehic. Tech. Conf. (VTC Fall), 2016, pp. 1-5.

[36] M. Yusuf and H. Arslan, "Enhancing Physical-Layer Security in Wireless Communications Using Signal Space Diversity," IEEE Military Commun. Conf. (MIL-COM), 2016.

[37] M. Yusuf and H. Arslan, "Secure Multi-User Transmission Using CoMP Directional Modulation," IEEE Vehic. Tech. Conf. (VTC Fall), 2015, pp. 1-2.

Appendix A

Average Probability of Bit Error for SSD System with Adaptive Interleaver

By substituting (3.11) and (3.12) into (3.13) we get

$$
P_s(k_1, k_2) = \frac{N!}{(k_1 - 1)!(N - k_1)!} \frac{N!}{(k_2 - 1)!(N - k2)!}
$$

$$
\int_0^\infty \int_0^\infty \int_0^{\frac{\pi}{2}} \frac{1}{\pi} \, e^{-\left(\dfrac{\alpha_1 d_I^2 + \alpha_2 d_Q^2}{2\sin^2\phi} \right)} d\phi \tag{A.1}
$$

$$
\left[1 - e^{-\alpha_1/\bar{\alpha}} \right]^{k_1 - 1} \left[e^{-\alpha_1/\bar{\alpha}} \right]^{N - k_1} \frac{1}{\bar{\alpha}} e^{-\alpha_1/\bar{\alpha}} d\alpha_1
$$

$$
\left[1 - e^{-\alpha_2/\bar{\alpha}} \right]^{k_2 - 1} \left[e^{-\alpha_2/\bar{\alpha}} \right]^{N - k_2} \frac{1}{\bar{\alpha}} e^{-\alpha_2/\bar{\alpha}} d\alpha_2
$$

where f_α and F_α in (3.12) are taken from (3.9) and (3.10) respectively. Using the binomial expansion we can get

$$
\begin{aligned}
P_s(k_1, k_2) = B \int\limits_0^{\frac{\pi}{2}} \int\limits_0^\infty \int\limits_0^\infty e^{-\alpha_1 \left(\frac{N-k_1+1}{\bar{\alpha}} + \frac{d_I^2}{2\sin^2\phi} \right)} \\
e^{-\alpha_2 \left(\frac{N-k_2+1}{\bar{\alpha}} + \frac{d_Q^2}{2\sin^2\phi} \right)} \sum_{u_1=0}^{k_1-1} \binom{k_1-1}{u_1} \left(-e^{-\alpha_1/\bar{\alpha}} \right)^{u_1} \\
\sum_{u_2=0}^{k_2-1} \binom{k_2-1}{u_2} \left(-e^{-\alpha_2/\bar{\alpha}} \right)^{u_2} d\alpha_1 d\alpha_2 d\phi
\end{aligned}
\tag{A.2}
$$

where

$$
B = \frac{1}{\pi\bar{\alpha}^2} \frac{N!}{(k_1-1)!(N-k_1)!} \frac{N!}{(k_2-1)!(N-k2)!}.
$$

Rearranging (A.2) gives us

$$
\begin{aligned}
P_s(k_1, k_2) = B \sum_{u_1=0}^{k_1-1} \sum_{u_2=0}^{k_2-1} \binom{k_1-1}{u_1} \binom{k_2-1}{u_2} (-1)^{u_1+u_2} \\
\int\limits_0^{\frac{\pi}{2}} \int\limits_0^\infty \int\limits_0^\infty e^{-\alpha_1 \left(\frac{u_1+N-k_1+1}{\bar{\alpha}} + \frac{d_I^2}{2\sin^2\phi} \right)} \\
e^{-\alpha_2 \left(\frac{u_2+N-k_2+1}{\bar{\alpha}} + \frac{d_Q^2}{2\sin^2\phi} \right)} d\alpha_1 d\alpha_2 d\phi
\end{aligned}
\tag{A.3}
$$

which we integrate over α_1 and α_2 to get

$$
\begin{aligned}
P_s(k_1, k_2) = \sum_{u_1=0}^{k_1-1} \sum_{u_2=0}^{k_2-1} \frac{2A}{\pi} \binom{k_1-1}{u_1} \binom{k_2-1}{u_2} (-1)^{u_1+u_2} \\
\int\limits_0^{\frac{\pi}{2}} \frac{\sin^4\phi}{(\sin^2\phi + \beta)(\sin^2\phi + \gamma)} d\phi
\end{aligned}
\tag{A.4}
$$

where A, β and γ are the same as in (3.14). The integral in (A.4) can be solved using partial fraction expansion as

$$I = \int_0^{\frac{\pi}{2}} \left[1 - \frac{\beta}{\beta - \gamma} \frac{\beta}{\sin^2\phi + \beta} + \frac{\gamma}{\beta - \gamma} \frac{\gamma}{\sin^2\phi + \gamma} \right] d\phi$$

$$= \frac{\pi}{2} \left[1 - \frac{\beta}{\beta - \gamma} \sqrt{\frac{\beta}{1 + \beta}} + \frac{\gamma}{\beta - \gamma} \sqrt{\frac{\gamma}{1 + \gamma}} \right] \qquad (A.5)$$

Substituting (A.5) into (A.4) gives the final result in (3.14).

Appendix B

Acronyms

CSI   channel state information

SSD   signal space diversity

OFDM   orthogonal frequency division multiplexing

TDD   time division duplex

CFO   carrier frequency offset

LOS   line of sight

DM   directional modulation

CoMP   coordinated multipoint

CR   clear region

ISI   inter symbol interference

DFE   decision feedback equalizer

CP   cyclic prefix

ICI   inter carrier interference

IFFT	inverse fast fourier transform
AWGN	additive white gaussian noise
FFO	fractional frequency offset
BER	bit error rate
PAPR	peak to average power ratio
SNR	signal to noise ratio
AN	artificial noise
ARQ	automatic repeat request
FFD	frequency division duplex
PSK	phase shift keying
QAM	quadrature amplitude modulation
I	in phase
Q	quadrature
PDF	probability density function
CDF	cumulative distribution function
MDDM	multiple directions directional modulation
BS	base station