ADVANCED CROSS-LAYER SECURE COMMUNICATION DESIGNS FOR FUTURE WIRELESS SYSTEMS

A DISSERTATION SUBMITTED TO

THE GRADUATE SCHOOL OF

ENGINEERING AND NATURAL SCIENCES

OF ISTANBUL MEDIPOL UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR

THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

ELECTRICAL, ELECTRONICS ENGINEERING AND CYBER SYSTEMS

By

Jehad M. Hamamreh

July, 2018

ABSTRACT

ADVANCED CROSS-LAYER SECURE COMMUNICATION DESIGNS FOR FUTURE WIRELESS SYSTEMS

Jehad M. Hamamreh
Ph.D. in Electrical, Electronics Engineering and Cyber Systems
Advisor: Prof. Dr. Hüseyin Arslan
July, 2018

Due to the inherent vulnerability of wireless transmission to eavesdropping, confidentiality arises as a challenging issue especially for future wireless networks because of their unique requirements. To cope up with this, physical layer security (PLS) has emerged as a new concept and prospective solution that can complement and even replace encryption-based methods, which entail many practical problems that may impede its implementation and adoption in future wireless networks. To address this challenge, in this thesis, novel, advanced and cross physical (PHY) and media access control (MAC) layer security designs are developed for providing confidentiality against eavesdropping in future wireless networks. The conducted research studies encompass the following main approaches. I) Cross PHY/MAC layer security techniques using: 1) Automatic-repeat-request (ARQ) with maximal ratio combination (MRC) and adaptive modulation; 2) ARQ with MRC and null-space-independent artificial noise. II) Security techniques for orthogonal frequency-division multiplexing (OFDM)-based waveforms. This includes developing new designs that cover the following topics: 1) OFDM with adaptive interleaving and precoding. 2) OFDM with subcarrier index selection for enhancing security and reliability of 5G services. 3) Cyclic prefix (CP)-less OFDM with alignment signals for enhancing spectral efficiency, reducing latency, and improving PHY security of 5G and beyond services. III) New inherently secure waveform designs, where a secure channel-based transform waveform, referred to as orthogonal transform division multiplexing (OTDM) waveform, is developed and proposed for future 5G wireless systems. Then, its time-frequency characteristics are investigated along with devising a method to reduce its peak-to-average power ratio. IV) Security designs for orthogonal space-time block coding (OSTBC)-based multi-input-single-output (MISO) systems, where precoding matrix indicators (PMI) are utilized and redesigned for providing secrecy.
Keywords: Physical layer security, OFDM, STBC, ARQ, MRC, MAC, PHY, 5G.

ÖZET

GELECEĞIN KABLOSUZ SISTEMLERINDE KATMANLAR ARASI İLERI GÜVENLI HABERLEŞME TASARİMLARİ

Jehad M. Hamamreh
Elektrik-Elektronik Mühendisliği ve Siber Sistemler, Doktora
Tez Danışmanı: Prof. Dr. Hüseyin Arslan
Temmuz, 2018

Kablosuz iletimde gönderilecek bilginin gizlice dinlenebilmesi, farklı ihtiyaç gereksinimlerine sahip gelecekteki haberleşme sistemleri için iletim güvenirliliğini zorlu bir sorun olarak ortaya çıkarmaktadır. Bununla başa çıkmak için fiziksel katman güvenliği (PLS) güçlü ve ileriye dönük yeni bir çözüm olarak ortaya çıkmıştır. Bu yöntem gelecek haberleşme sistemlerinde uygunabilirlik açısından problemler oluşturabilecek şifreleme tabanlı yöntemleri tamamlayabilir, hatta yerini alabilir. Bu tezde, bahsi geçen problemi çözmek için özgün ileri ve çapraz PHY/MAC katman güvenlik tasarımları yapıldı. Geliştirilen yöntemlerin yeni nesil haberleşme sistemlerinde gizlice dinlenilmeye karşı güvenirliliği artıracağı ortaya koyuldu. Yapılan araştırma çalışmaları aşağıdaki ana yaklaşımları kapsamaktadır. I) Çapraz PHY/MAC katman güvenlik teknikleri: 1) Maksimum oran kombinasyonu (MRC) ve adaptif modülasyon ile otomatik-tekrar-istek (ARQ); MRC ve boşluk uzayından bağımsız yapay gürültü ile ARQ. II) OFDM tabanlı dalga formları için güvenlik teknikleri. Yeni tasarımlar kapsamında yürütülmüş faaliyetler şunlardır: 1) Uyarlamalı serpiştirme ve ön kodlama ile OFDM. 2) 5G URLLC hizmetlerinde güvenlik ve güvenilirliğin arttırılması için alt taşıyıcı indeks seçimi ile OFDM. 3) Spektral verimliliği arttırmak, gecikmeyi azaltmak ve PHY güvenliğini geliştirmek için hizalama sinyalleri ile ön-eksiz (CP-less) OFDM. III) Dikgen dönüşüm bölmeli çoğullama (OTDM) olarak adlandırılan güvenli kanal tabanlı dönüşüm dalga form tasarımları gelecek haberleşme sistemleri için geliştirildi ve önerildi. Daha sonra, bu dalga formunun zaman-frekans karakteristiği incelendi, zirve ve ortalama güç oranını (PAPR) düşürmek için bir yöntem geliştirildi. IV) MISO tabanlı dikgen uzay-zaman blok kodlamalı (OSTBC) sistemler için ön gösterge matris göstergelerinin (PMI) kullanıldığı ve yeniden tasarlandığı güvenlik tasarımları sunuldu.

Anahtar sözcükler: Fiziksel katman güvenliği, OFDM, STBC, ARQ, MAC, PHY.

Acknowledgement

First, I extend my gratitude and thanks to Allah (swt) for everything that He granted me in this life. I would like to express my thanks to my advisor Dr. Huseyin Arslan for his guidance, motivation, and support throughout my study. I wish also to thank Dr. Tuncer Baykas, Dr. Ertugrul Basar, Dr. Ercumend Arvas, and Dr. Ali Gorcin for serving in my committee and for offering valuable suggestions and constructive comments. I hope to be able to benefit from their deep, thorough knowledge and unique, wide experience; and to also continue collaborating with them in the future as well.

It has been a privilege to be a research assistant member of the Communication, Signal processing and Networking Center (CoSiNC) at Istanbul Medipol University, where I have acquired both knowledge and experience in the field of wireless telecommunication systems through being involved in many high-tech, challenging, yet exciting research projects.

I would like to thank all my friends in both CoSiNC group (IMU in Turkey) and WCSP group (USF in USA) for their support and faithful advices as friends and productive, fruitful discussions as colleagues.

Last, but not least, I would like to express my deepest gratitude to my parents, brothers and sisters for their unconditional, continuous, and encouraging support throughout these years.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

Wireless communication services are enormously increasing day by day as a consequence of the massive spread in wireless devices featured by high mobility and ease of use. Moreover, the surge in wireless data communication is primarily driven by the huge amount of beneficial applications customized for mobile users. Since wireless media is becoming the dominant access for most of the Internet-based services, serious security risks appear on the service-carrying wireless signals and waves because of their broadcast nature. Thus, new security requirements have urgently been demanded. Specifically, users require confidential transmission for their generated wireless data, such as their important sensitive messages, calls, videos, financial transactions, etc. As a matter of fact, strongly secure communication systems are desirable to be implemented without just relying on the traditional cryptographic key-based sharing approaches, which are mostly dependent on Shannon's security model [3].

Physical layer security (PLS) [4], the third driving factor for research after capacity and reliability, emerges as a promising and revolutionizing concept to address the eavesdropping security problem [5–8]. The driving motivations behind PLS research can be summarized by the following five practical security

problems.

First, the key management, distribution, and maintenance processes for the legitimate parties are extremely challenging, especially in large-scale heterogeneous and decentralized wireless networks. **Second**, longer key length, which is desirable to increase the confidentiality level, results in more waste of resources, which are needed for sharing, storing and managing the keys properly. In addition, it is not surprising that implementing and adopting security methods that achieve Shannon's perfect secrecy[1] using one time pad method, which requires secret key of length equal to the data itself, is impractical in today's data volume. **Third**, the fast advances and developments in electronics and processing and computing power devices reveal the fact that current secret key-based techniques, which are based on the assumption that the eavesdropper has limited computational power capabilities, can be cracked, no matter how much mathematically complex they are, especially when quantum computing and quantum communication becomes a reality. **Fourth**, the emergence of new wireless technologies like Internet of Things (IoT), massive machine-type communication (mMTC), 5G-Tactile Internet, vehicular communication for autonomous driving, remote surgery, instant control for sensitive IoT actuators, etc. makes current encryption-based methods unsuitable since these kind of technologies are naturally delay-sensitive, power-limited, and processing-restricted. **Fifth**, users with sensitive applications like those related to financial and personal secret information can never compromise security, even if it becomes at the expense of slight degradation in other performance measures like throughput and reliability. In the near future, users are anticipated to even be willing and ready to pay extra charges just for the sake of completely ensuring the security of their important services. Thus, Physical Security as a Service (PSaaS) is expected to be one of the future coming killer applications for mobile service providers, where users can be charged a little more for providing them with strong, perfect secure services.

[1]It is an information-theoretic notion which indicates the highest security level, where the secrecy capacity is equal to the capacity of the main channel for key-less-based methods or the length of the secret key is equal to the length of the transmitted data for key-based methods, resulting in a perfect secrecy in which there is no information leakage to Eve.

The aforementioned issues and challenges inspire and motivate the development and production of new, practical, efficient security schemes that can work at the lower physical (PHY) and MAC layers to protect the wireless transmissions from passive eavesdropping.
In this thesis, we propose new effective security methods by redesigning and exploiting some of the key enabling technologies of current and future wireless systems such as advanced automatic-repeat-request (ARQ), multicarrier waveforms, and multi antenna transmission. The proposed security techniques guarantee a very suitable security level against eavesdropping by exploiting the functionalities of the PHY and MAC layers. This is achieved while trying to efficiently utilize the proposed design to also enhance the performance of other important metrics such as reliability, spectral efficiency, peak-to-average power ratio (PAPR) and out of band emission (OOBE).

1.2 Scope of the Thesis

The scope of this thesis is to design and develop effective security techniques by the joint exploitation of PHY and MAC layers functionalities to protect the wireless transmission against eavesdropping. The chapters include detailed description of the considered scenarios, proposed security methods and designs, performance evaluation results of the proposed designs and comparisons with the existing ones in the literature. Particularly, this thesis work spans and encompasses the following main directions: 1) cross PHY/MAC layer security: a) ARQ with MRC and adaptive modulation. b) ARQ with MRC and null-space-independent artificial noise. 2) Security technique for OFDM-based waveforms. a) Adaptive precoding (interleaving) and postcoding (deinterleaving) for OFDM. b) OFDM with subcarrier index selection. c) CP-less OFDM with signal alignment. 3) New inherently secure waveform designs. 4) Security in OSTBC MISO systems. 5) Comprehensive literature survey of the state of the art on the techniques, applications and metrics used in secure signal transmission.

1.3 Thesis Contributions

The main contributions of the research studies conducted during my PhD period include and encompass the following main topics related to the field of wireless communication security.[2]

- Cross PHY/MAC layer security.

    1. ARQ with adaptive modulation. In this work, Automatic-Repeat-Request (ARQ) and Maximal Ratio Combination (MRC), have been jointly exploited to enhance the confidentiality of wireless services requested by a legitimate user (Bob) against an eavesdropper (Eve). The obtained security performance is analyzed using Packet Error Rate (PER), where the exact PER gap between Bob and Eve is determined. PER is proposed as a new practical security metric in cross layers (Physical/MAC) security design since it reflects the influence of upper layers mechanisms, and it can be linked with Quality of Service (QoS) requirements for various digital services such as voice and video. Exact PER formulas for both Eve and Bob in i.i.d Rayleigh fading channel are derived. The simulation and theoretical results show that the employment of ARQ mechanism and MRC on a signal level basis before demodulation can significantly enhance data security for certain services at specific SNRs. However, to increase and ensure the security of a specific service at any SNR, adaptive modulation is proposed to be used along with the aforementioned scheme. Analytical and simulation studies demonstrate orders of magnitude difference in

[2]It should be mentioned that throughout the numerous contributions that we make and report in this thesis pertaining to the field of communication security, there are also other valuable contributions related to providing enhancements in other important performance metrics such as: 1) reliability and power efficiency as it can be noticed in OTDM waveform related work and OFDM-SIS related study as well; 2) spectral efficiency as it can be perceived in CP-less OFDM related work; 3) peak-to-average power ratio (PAPR) and out-off-band emission (OOBE) as it can be seen in ARQ related work and OTDM-related work as well. Accordingly, one can clearly see that this dissertation is very different from the other available ones in the literature of physical layer security in the sense that it enhances note only secrecy but also other important performance metrics.

PER performance between eavesdroppers and intended receivers.

2. ARQ with null-space-independent, adaptive and PAPR-aware artificial noise. Automatic-repeat-request (ARQ) as a MAC layer mechanism and artificial noise (AN) as a physical layer (PHY) mechanism along with the help of maximal ratio combining (MRC), are jointly designed to achieve secrecy. Basically, a special AN, which does not require null-space in the channel, is designed based on the quality of service (QoS) requirements and the channel condition between the legitimate parties and injected to the data packet. If the same packet is requested by the legitimate receiver (Bob), an AN canceling signal is properly designed and added to the next packet. Then, an AN-free packet is obtained by using MRC process at Bob, while deteriorating the eavesdropper performance. Furthermore, two simple closed-form expressions of the achievable secure throughput are derived. The first one is given in a closed-form for the case of ARQ scheme without AN, while the second one is given in an upper-bound form for the case of ARQ with AN. Moreover, this work addresses two critical security-associated problems: (i) the joint design of secrecy, reliability, throughput, delay and the trade-off among them, and (ii) the increase in the peak-to-average power ratio (PAPR) due to the added AN.

3. Utilizing the proposed design to control PAPR and OOBE in OFDM design, while maintaining secrecy. The aforementioned proposed design is extended to OFDM to demonstrate its capability in not only enhancing the secrecy due to the frequency selectivity of the channel, but also in reducing the PAPR and out-of-band emission (OOBE) of OFDM-based waveforms, while maintaining secrecy.Two optimization problem are formulated and solved using numerical optimization solvers.

- Security technique for OFDM-based waveforms.

1. Secure precoding and postcoding (adaptive interleaving and deinterleaving) for OFDM systems along with hardware implementation. In this study, an effective and hardware-friendly physical layer security

design composed of a channel-based frequency pre- coder and a post-coder for OFDM-based systems is proposed. The design is achieved by decomposing the diagonal matrix of the channel frequency amplitude of the legitimate receiver in order to obtain two unitary orthonormal matrices. The first matrix is used as a pre-coder just before the IFFT process at the transmitter, while the second matrix is used as a post-coder just after the FFT process at the receiver. Besides security, the presented design is interestingly found out to work as a shuffler or interleaver, which does not only provide secrecy, but also enhances the performance against burst errors. Moreover, a new channel calibration technique is developed to overcome the effect of channel reciprocity mismatch on the proposed scheme. The provided simulations and USRP hardware testbed implementation results validate the effectiveness of the proposed design in achieving practical and reliable secrecy with minor modifications on the OFDM structure.

2. OFDM-Subcarrier Index Selection for Enhancing Security and Reliability of 5G URLLC Services. An efficient physical layer security technique, referred to as OFDM with subcarrier index selection (OFDM-SIS), is proposed for safeguarding the transmission of OFDM-based waveforms against eavesdropping in 5G and beyond wireless networks. This is achieved by developing a joint optimal subcarrier index selection (SIS) and adaptive interleaving (AI) design, which enables providing two levels (sources) of security in time division duplexing (TDD) mode: one is generated by the optimal selection of the subcarrier indices that can maximize the signal-to-noise ratio (SNR) at only the legitimate receiver, while the other is produced by the AI performed based on the legitimate user's channel that is different from that of the eavesdropper. The proposed scheme not only provides a remarkable secrecy gap, but also enhances the reliability performance of the legitimate user compared to the standard OFDM scheme. Particularly, a gain of 5-10 dB is observed at a bit error rate (BER) value

of $10^{-}3$ compared to standard OFDM as a result of using the adaptive channel-based subcarrier selection mechanism. Moreover, the proposed technique saves power, considers no knowledge of the eavesdropper channel, and provides secrecy even in the worst security scenario, where the eavesdropper can know the channel of the legitimate link when an explicit channel feedback is used as is the case in frequency division duplexing (FDD) systems. This is achieved while maintaining low complexity and high reliability at the legitimate user, making the proposed scheme a harmonious candidate technique for secure 5G ultra-reliable and low-latency communications (URLLC) services.

3. CP-Less OFDM with Alignment Signals for Enhancing Spectral Efficiency, Reducing Latency, and Improving PHY Security of 5G and Beyond Services. Although OFDM is a widely accepted waveform in many standards and is expected to keep its dominance in future 5G systems with various types of parametrized waveforms, its performance in terms of spectral efficiency as well as transmission latency is usually degraded due to the excessive usage of cyclic prefix (CP). Particularly, in highly dispersive channels, CP rate might be very large in order to maintain the low complex frequency domain equalization. In this paper, we propose a novel method that can fit the low latency and high spectral efficiency requirements of future 5G wireless services by eliminating the need for inserting CP between successive OFDM symbols while keeping the whole detection process the same at the receiver side. In order to achieve that, we utilize specially designed alignment signals that can cancel the interference of one symbol on the other and add an additional signal component that makes the signal circularly convolved with the channel at the receiver side. Simulation results prove the superiority of the proposed scheme in terms of enhancing spectral and power efficiency, reducing latency, and improving physical layer security against eavesdropping while using low complexity one tap frequency domain equalizer. These numerous, simultaneous, and desirable advantages have the potential to make the proposed technique a perfect fit for future 5G and beyond wireless services and

applications including IoT-based mMTC, URLLC, and eMBB.

- New secure waveform designs.

    1. Secure orthogonal transform division multiplexing (OTDM) waveform for 5G and beyond. In this work, a secure waveform design for future 5G wireless systems is proposed. The developed waveform, referred to as secure orthogonal transform division multiplexing (OTDM) waveform, is designed to diagonalize the multi-path channel matrix of only the legitimate receiver (Bob), while degrading eavesdropper reception. In particular, instead of using fixed exponential basis functions, generated by IFFT and FFT as in OFDM, orthogonal transform basis functions, which are extracted from the channel, are utilized to modulate and demodulate the data symbols. The simulation results prove that the proposed design provides a significant practical security gap between Bob's and Eve's performance. The design is shown to be robust against channel imperfection, and it neither sacrifices communication resources nor considers any knowledge on the eavesdropper channel. Besides security, the scheme results in a higher SNR, leading to a 3-5 dB gain over OFDM at BER=10^{-3}.
    2. Time-Frequency Characteristics and PAPR Reduction of OTDM Waveform. This paper provides an in-depth investigation and analysis on the characteristics of channel-based transform waveforms and their differences from Fourier transform-based waveforms. Particularly, the basis functions of the recently proposed orthogonal transform division multiplexing (OTDM) waveform, which belongs to the category of channel-based transform waveforms, are comprehensively compared with the fixed exponential basis functions of orthogonal frequency division multiplexing (OFDM) waveform, which pertains to the class of Fourier transform-based waveforms. The obtained results show significant differences in the time and frequency characteristics of both classes of the waveforms. Also, the peak-to-average power ratio (PAPR) of OTDM is investigated and compared to OFDM. Then, a

new effective technique, referred to as OTDM with edge subcarrier dedication (OTDM-ESD), is proposed for PAPR reduction by exploiting the special characteristics of the effective channel response in OTDM waveform. Simulation results show that the proposed OTDM-ESD technique not only reduces the PAPR, but also enhances the BER performance significantly.

- Security in OSTBC MISO systems. In this study, the secrecy performance obtained by employing precoded orthogonal space time block coding method (POSTBC) in MISO wireless networks is first investigated and quantified. In this scheme, space time codewords are precoded with an optimum matrix that minimizes the error rate at only the legitimate user (Bob). The acquired results depict that there exists a security gap region in the resulting BER performance as a consequence of using POSTBC, which selects an optimum precoding matrix that minimizes the BER at only Bob. Moreover, the performance of POSTBC scheme is enhanced more by developing a new hybrid and green security method called precoding along with partial pre-equalizing (PCPPE). In this method, the transmitted symbols are precoded by a new precoder composed of both the original precoder and a new designed unitary matrix that maps Bob's channel amplitudes or phases estimated over the transmitting antennas into 2D orthonormal matrix. Additionally, three issues associated with the proposed security method have been tackled. The comparative simulation results prove that PCPPE method provides a secure link among the legitimate parties without sacrificing Bob's reliability although an eavesdropper is assumed to be fully aware of the used method and the original selected precoding matrix indicator (PMI). The effect of imperfect channel estimation and reciprocity mismatch is also investigated.

- Classification and Applications of Physical Layer Security Techniques against Eavesdropping: A Comprehensive Survey. In this survey, we propose a conceptual and tractable framework for classifying the existing physical layer security techniques against wireless passive eavesdropping. In this

flexible framework, security techniques are divided into two primary approaches: SINR-based approach and complexity-based approach. The first approach is classified into three major categories: first, secrecy channel codes-based schemes; second, security techniques based on channel adaptation; third, schemes based on injecting intentional interfering signals into the transmitted information signals. The second approach, which is associated with the mechanisms of extracting secret sequences from the shared channel, is classified into one main technique called channel quantization. The implementation of each one of these categories is divided and classified into three main signal domains: time, frequency and space. For each one of these domains, several examples are given and illustrated along with the review of most recent security advances in each domain. Moreover, the advantage and disadvantages of each technique are discussed to give an insight on the trade-off process between security and the other communication requirements such as reliability, capacity, power efficiency, and complexity. The recent applications of physical layer security techniques into emerging areas like VLC, BAN, PLC, IoT, smart grid, mm-Wave, cognitive radio, vehicular, and 5G systems including secure waveforms and multiple accessing, are also reviewed and discussed. The paper is concluded with recommendations and future directions for designing robust, power-efficient and strong security methods for current and future wireless systems.

1.4 Thesis Outline

This thesis consists of nine chapters in which Chapter 1 provides the motivation, scope, contributions and outline of the thesis. In Chapter 2, we present a deep, detailed overview of physical layer security concept, system model, secrecy notions and metrics, classification of the security techniques and their applications in various wireless communication systems. In Chapter 3, we introduce the joint, cross PHY/MAC layer security design using ARQ with adaptive modulation and null-space independent, PAPR-aware artificial noise. Then in Chapter 4, we exhibit the details of OFDM with subcarrier index selection technique for enhancing

security and reliability of 5G URLLC services. In Chapter 5, we present CP-less OFDM design with alignment signals for enhancing spectral efficiency, reducing latency, and improving PHY security of 5G and beyond services. Chapter 6 illustrates the design of a new secure waveform for 5G and beyond named as Orthogonal Transform Division Multiplexing (OTDM) Waveform. In Chapter 7, the time-frequency characteristics of OTDM waveform are deeply investigated and a PAPR reduction technique for OTDM Waveform is explained. In Chapter 8, An effective, physical layer security method for precoded orthogonal space time block coding (OSTBC)-based systems is introduced. Finally, Chapter 9 concludes the thesis along with providing possible future research directions and recommendations.

1.5 Publications

Published Journals:

1. J. M. Hamamreh and H. Arslan, "Joint PHY/MAC Layer Security Design Using ARQ with MRC and Null-Space Independent, PAPR-Aware Artificial Noise in SISO Systems," IEEE Transactions on Wireless Communications, vol. 99, no. 99, pp. 1-15, 2018.

2. J. M. Hamamreh and H. Arslan, "Secure orthogonal transform division multiplexing (OTDM) waveform for 5G and beyond," IEEE Communication Letter, vol. 22, no. 5, pp. 1191-1194, Jan. 2017.

3. J. M. Hamamreh, E. Basar, and H. Arslan, "OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services," IEEE Access, vol. 5, pp. 25 86325 875, 2017.

4. E. Guvenkaya, J. M. Hamamreh, and H. Arslan, "On physical-layer concepts and metrics in secure signal transmission," Physical Communication by Elsevier, vol. 25, pp. 14 25, Aug. 2017.

5. A. M. Jaradat, J. M. Hamamreh and H. Arslan, "OFDM with subcarrier number modulation," IEEE Wireless Communications Letters, May. 2018.

Published Conference Papers:

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

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

3. J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Secure Pre-coding and Post-coding for OFDM Systems along with Hardware Implementation," in Proc. 2017 13th Intern. Wireless Commun. Mob. Comput. Conf. (IWCMC), June 2017, pp. 1338-1343.

4. J. M. Hamamreh and H. Arslan, "Time-Frequency Characteristics and PAPR Reduction of OTDM waveform for 5G and beyond," 2017 10th International Conference on Electrical and Electronics Engineering (ELECO), Bursa, 2017, pp. 681-685.

5. J. M. Hamamreh, Z. E. Ankarali, H. Arslan, "CP-Free OFDM Waveform with Alignment Signals," 2018 52st Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA, 2018, pp. 1-6. (Invited).

6. H. M. Furqan, J. M. Hamamreh, H. Arslan, "Secure Communication via Untrusted Switchable Decode-and-Forward Relay," IEEE International Wireless Communications and Mobile Computing Conference (IWCMC), 1-4, June 26-30, 2017.

7. H. M. Furqan, J. M. Hamamreh, H. Arslan, "Secret Key Generation Using Channel Quantization with SVD for Reciprocal MIMO Channels," in 2016 IEEE International Symposium on Wireless Communication Systems (ISWCS), Sep. 2016.

8. H. M. Furqan, J. M. Hamamreh, H. Arslan, "Enhancing Physical Layer Security of OFDM-based Systems Using Channel Shortening," IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Oct. 8-13, 2017.

Journals Under Review:

1. J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and Applications of Physical Layer Security Techniques against Eavesdropping: A Comprehensive Survey," Submitted to IEEE Communications Surveys and Tutorials, PP. 1-50, 2018. (Decisioned with Revise and Resubmit).

2. H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Adaptive OFDM-IM for Enhancing Physical Layer Security and Spectral Efficiency," Submitted to Hindawi Wireless Communications and Mobile Computing, Special Issue on Safeguarding 5G Networks through Physical Layer Security, 2018. (Minor Revision, Second Round).

3. J. M. Hamamreh, Z. E. Ankarali, and H. Arslan, "CP-Less OFDM with Alignment Signals for Enhancing Spectral Efficiency, Reducing Latency, and Improving PHY Security of 5G and Beyond Services," Submitted to IEEE Access, 2018.

4. A.M, Jaradat, J. M. Hamamreh, and H. Arslan, "Modulation Options for OFDM Waveform," to be submitted to IEEE Communication Magazine, 2018.

5. J. M. Hamamreh, and H. Arslan, "OFDM-Subcarrier Index Selection with Artificially Interfering Signals for Enhancing PHY Security," to be submitted to Physical Communication, 2018.

Patents:

1. J. M. Hamamreh, H. Arslan, "A Secure, Adaptive Orthogonal Division Waveforms Multiplexing System Using Channel-Based Transformation", U.S. and Turkish Patent, 2016.

2. J. M. Hamamreh, H. Arslan, "Automatic Repeat Request (ARQ) with Superimposed Interfering Signals for Providing Absolute Confidentiality and Authentication in Wireless Networks", Turkish Patent App. 2017.

Chapter 2

Classifications and Applications of Physical Layer Security Techniques against Eavesdropping

2.1 Background, Motivation, Contributions and Organization

Wireless communication services are enormously increasing day by day as a consequence of the massive spread in wireless devices featured by high mobility and ease of use. Moreover, the surge in wireless data communication is primarily driven by the huge amount of beneficial applications customized for mobile users. Since wireless media is becoming the dominant access for most of the Internet-based services, serious security risks appear on the service-carrying wireless signals and waves because of their broadcast nature. Thus, new security requirements have urgently been demanded. Specifically, users require confidential transmission for their generated wireless data, such as their important sensitive messages, calls,

videos, financial transactions, etc. As a matter of fact, strongly secure communication systems are desirable to be implemented without just relying on the traditional cryptographic key-based sharing approaches, which are mostly dependent on Shannon's security model [3].

To this end, physical layer security (PLS) [4], the third driving factor for research after capacity and reliability, emerges as a promising and revolutionizing concept to address the eavesdropping security problem [5–8]. The driving motivations behind PLS research can be summarized by the following five practical security problems.

First, the key management, distribution, and maintenance processes for the legitimate parties are extremely challenging, especially in large-scale heterogeneous and decentralized wireless networks. **Second**, longer key length, which is desirable to increase the confidentiality level, results in more waste of resources, which are needed for sharing, storing and managing the keys properly. In addition, it is not surprising that implementing and adopting security methods that achieve Shannon's perfect secrecy[1] using one time pad method, which requires secret key of length equal to the data itself, is impractical in today's data volume. **Third**, the fast advances and developments in electronics and processing and computing power devices reveal the fact that current secret key-based techniques, which are based on the assumption that the eavesdropper has limited computational power capabilities, can be cracked, no matter how much mathematically complex they are, especially when quantum computing and quantum communication becomes a reality. **Fourth**, the emergence of new wireless technologies like Internet of Things (IoT), massive machine-type communication (mMTC), 5G-Tactile Internet, vehicular communication for autonomous driving, remote surgery, instant control for sensitive IoT actuators, etc. makes current encryption-based methods unsuitable since these kind of technologies are naturally delay-sensitive, power-limited, and processing-restricted. **Fifth**, users with sensitive applications like those related to financial and personal secret information can never compromise

[1]It is an information-theoretic notion which indicates the highest security level, where the secrecy capacity is equal to the capacity of the main channel for key-less-based methods or the length of the secret key is equal to the length of the transmitted data for key-based methods, resulting in a perfect secrecy in which there is no information leakage to Eve.

security, even if it becomes at the expense of slight degradation in other performance measures like throughput and reliability.

The story of modern security starts from Shannon, who laid down the foundation of secrecy systems in his seminal paper [3]. Although Shannon-based works (i.e., cryptography-based methods that assume noiseless channel at both the legitimate and eavesdropper sides) have dominantly been applied to secure communication systems using shared secret keys, they have got serious drawbacks and issues, which are basically the motivations for the PLS research. These issues are basically the aforementioned first four points summarized in the previous paragraphs.

As a consequence of the many issues associated with cryptographic-based security, key-less information-theoretic security has emerged as a desirable and promising solution to address most (if not all) of the aforementioned issues. In Wyner's work [4], which constitutes the foundation and starting point of the research on PLS, it was explained that confidential communication between legitimate users is possible without sharing a secret key if the eavesdropper's (Eve's) channel is a degraded (much noisier) version of the intended receiver's (Bob) channel. Accordingly, channel-dependent stochastic encoders, which generate random secrecy codes, were used to achieve confidentiality by exploiting the channel without using shared secret keys.

Similar to Shannon-based works, Wyner-based studies have also obtained their own drawbacks and limitations, which can be summarized as follows: 1) Eve is always assumed to have a degraded channel compared to Bob, i.e., Eve's signal-to-interference-and-noise ratio (SINR) must be lower than that of Bob. However, In practical scenarios, due to the uncertain location, random fading, and broadcast nature of the wireless channel, Eve's channel condition, represented by the SINR, can be comparable to or even better than Bob's one, especially when Eve is closer to the transmitter than Bob; therefore, Wyner-based methods become inapplicable in such scenarios. 2) Secrecy can be achieved in most cases at the expense of capacity and throughput reduction (i.e., there is an intrinsic trade-off between capacity and secrecy). 3) The method is basically designed to merely

secure messaging service, but not voice, video, and other services, whose quality of service (QoS) requirements are different from messaging service.

Inspired by Wyner's work, the characterization and investigation of the achievable secrecy capacity against eavesdropping were studied from an information-theoretic point of view for different channel types, communication scenarios, and under various assumptions on the availability of channel state information (CSI). These studies were extensively surveyed and reported in several recent survey papers [6–9] and books on physical layer security [10–14].

Motivation: We have thoroughly explored and investigated the aforementioned elegant surveys alongside other topic-specific tutorials [5, 15–26]; and noticed that most of these surveys review the previously published studies on PLS based on communication scenarios, channel types and conditions, or system configurations (with more focus on information theoretical studies) with the goal to span and cover most of the research papers published on PLS in an inclusive methodological manner. More precisely, in most of the available well-known PLS surveys such as [6,7,22], and [9], one can clearly notice that the common structure adopted in reviewing the PLS papers available in the literature is more or less scenario-dependent, where the studies are divided into different wiretap channels and scenarios of the following main types: 1) single antenna, 2) multi-antenna, 3) relay, 4) multiuser broadcast, 5) multiaccess, 6) interference, and 7) large scale heterogeneous cognitive networks, which may include different combinations of various channel types. Although such a structural review that is channel type and scenario-dependent might ease the review of papers, it unfortunately does not clearly classify and identify in a generic conceptual manner the underlying transmission strategies that are responsible for providing secrecy against eavesdropping in any considered scenario (i.e., scenario-independent).

Moreover, the applications of PLS to some of the emerging wireless systems and technologies such as visible light communication (VLC), body area network (BAN), power line communication (PLC), radio frequency identification (RFID), Internet of things (IoT), device-to-device (D2D), vehicular ad hoc network (VANET), smart grid, ultra-wide-band (UWB), unmanned aerial vehicle

(UAV), mm-Wave, cognitive radio, index modulation, and new multiple accessing schemes like non-orthogonal multiple access (NOMA) have been intensifying within the last few years. Thus, it is very significant and worthy to review the most recent state of the art on these important emerging systems that are already being adopted in practice, not only to make the community aware of the research studies that have been conducted in each domain, but also to facilitate understanding the specific requirements imposed on PLS techniques when being applied and adopted in these domains alongside manifesting new research opportunities and directions.

Contribution: Motivated by these observations, in this chapter, we first focus our attention on establishing and structuring a unique and unified taxonomy framework that can classify and fit all the existing physical layer security techniques proposed in the literature under one big comprehensive umbrella in a very conceptual, expandable, and easily understandable way. This framework is anticipated to help researchers, engineers, cyber-security practitioners, system designers, students, and interested public from both industry and government sectors in clearly grasping the big picture of physical layer security. Particularly, this framework enables new researchers in this field to easily and quickly catch up with the state of the art, realize the kernel concept behind the enabling security techniques, their advantages and disadvantages, the used secrecy metrics and notions, and how to develop new ones based on the requirements of the applications and services that are targeted to be secured[2].

Besides, it clearly states the learned lessons, remarks, merits, and demerits of the various introduced security methods in the literature so that security designers can know what kind of techniques is more suitable to be used in a certain scenario under specific constraints and requirements. Additionally, with the help of the proposed framework, researchers can solidify their efforts on trying to maximize and maintain the merits of each security technique, while minimizing or even fully overcoming its demerits and drawbacks.

[2]Note that since this survey is intended to be exclusively devoted to comprehensively review the state of the art **techniques** of physical layer security alongside their classifications and applications, the review of information theory and performance analysis related studies is kept at minimal (i.e., these kind of studies are reviewed briefly wherever is need in this survey to support the concept and features of the discussed techniques).

The second exciting part of this survey is the comprehensive discussion and review of the recent applications of PLS to many of the emerging communication systems such as VLC, BAN, PLC, RFID, IoT, D2D, VANET, UWB, UAV, NOMA, mm-Wave, smart grid, cognitive radio, and index modulation-based systems. This inclusive review sheds the light on the implications of employing PLS concepts to these systems and how security designs may require to be deliberately modified according to new requirements and constraints determined by the characteristics of such systems.

Organization: The organizational structure of this chapter proceeds as follows. Section 2.2 explains the generic system model and main preliminaries of the considered eavesdropping PLS problem. Section 2.3 presents and categorizes the secrecy notions and metrics used in PLS to characterize and quantify secrecy performance. Section 2.4 explains and classifies the techniques related to the approach of SNR-based PLS into three major categories: First, secrecy channel codes-based schemes; second, security techniques based on channel adaptation; third, schemes based on injecting intentionally well-designed interfering (noise/jamming) signals alongside the transmitted information signals. The second approach, which is associated with the mechanisms of extracting secret sequences (keys) from the shared channel, is classified into two main categories based on which layer the secret sequence obtained by channel quantization is applied on. The enabling security techniques pertaining to each one of these categories are divided into three main signal domains: time, frequency and space. For each one of these domains, several examples are given and illustrated along with the review of most recent security advances in each domain. Section 2.5 exhibits the applications of PLS to emerging areas like VLC, BAN, PLC, IoT, smart grid, mm-Wave, cognitive radio, vehicular, UAV, UWB, D2D, RFID, and 5G systems including secure index modulation waveforms and NOMA-based security designs.

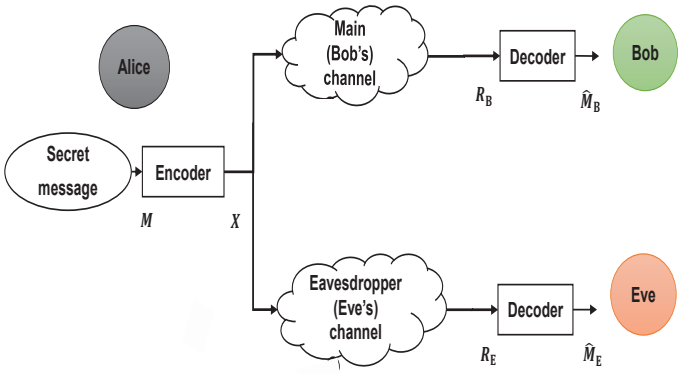


Figure 2.1: Generic system model of physical layer security related to eavesdropping problem, in which Alice tries to communicate confidentially with Bob without allowing Eve to get any useful information from the ongoing communication between the legitimate parties (Alice and Bob).

2.2 System Model and Preliminaries

In the generic model of physical layer security problem, we usually have three main communication entities (nodes) as depicted in Fig. 2.1. The first node is basically the legitimate transmitter node, and is referred to as Alice. The second node is the legitimate receiver node, and is referred to as Bob, while the third node, named as Eve, is the malicious eavesdropper node. In this setup, Alice aims at sending secret data content and communicating confidentially with Bob in the presence of Eve that tries to intercept the ongoing communication between the legitimate parties (Alice and Bob). In other words, Eve's target is to decode and obtain the secret data content from her own observations of the received signals. Accordingly, the goal of Alice is to device and use a transmission technique or method that can deliver the secret data messages intact to Bob, while making sure that Eve is kept ignorant and unable to decode the transmitted secret messages. To achieve secrecy in such scenario, PLS techniques are properly designed via exploiting the channel characteristics including noise, fading, interference, dispersion, diversity, etc., along with the transceiver architecture including synchronization, estimation, hardware impairments, etc., in order to make the data transmission in favor of Alice only, and thus overcoming the eavesdropping problem.

As presented in Fig. 2.1, the confidential information message, M, is encoded into X of length n, and then sent through a wireless channel. The received signals at Bob and Eve are indicated by R_B and R_E, respectively. The entropy of the source information is given by $H(M)$, whereas the residual uncertainty (conditional entropy) for the eavesdropper's observation is denoted by $H(M|R_E)$. Now, based on the scenario and environment under consideration, the availability of channel state information (CSI) at the communication parties varies from complete to partial to even zero knowledge. However, in a practical wireless system, all communication parties can acquire some information about the channel between the transmitter and themselves.

Moreover, Alice is usually assumed to know the CSI of the legitimate receiver by the means of exploiting the reciprocity of the channel in a time division duplexing (TDD) system or by receiving CSI feedback from Bob in a frequency division duplexing (FDD) system. Furthermore, in spite of the fact that Alice has to practically be assumed to have no knowledge about Eve's channel as she is usually passive (i.e., not communicating with the other nodes in the systems, just listening); one can find in the literature that Alice is sometimes assumed to know Eve's channel [27] [28] [29]. This is justified by the fact that Eve can be considered a licensed user who has legal access to the network, but has a bad intention in eavesdropping the communication of other users in the network. One final notice to mention is the reality that Eve's and Bob's channels are usually assumed to be independent of each other due to the spatial de-correlation property of the wireless channel response (i.e., channels de-correlate and become independent from each others if they are half wavelength apart from each other).

2.3 Secrecy Notions and Performance Metrics

2.3.1 Secrecy Notions

In the literature of PLS, there are several common secrecy notions, which are frequently used by researchers as design criteria intended to describe the level of security that a certain scheme or method can provide. In fact, there has been a controversial debate about the exact interpretation of some of these notions such as perfect secrecy, strong secrecy and weak secrecy [30]. Shannon-based works define perfect secrecy to be exactly equal to the legitimate receiver capacity (main channel capacity) when Eve's channel capacity (wire-tap capacity) exactly equals zero, i.e., zero information leakage to Eve; for any code length. This definition is modified when the code length tends to infinity, and this results in what is called strong secrecy when the code length is sufficiently long enough. On the other hand, Wyner-based works considered secrecy to be perfect if and only if the secrecy capacity has a positive value with a certain probability, no matter how much small this value might be and regardless of Eve's capacity or the amount of information that leaks to Eve. Thus, this definition results in what is called weak secrecy, in which there exists a rate (usually small and affected by SNR) at which perfect communication can be achieved. Besides the notions of perfect, strong, and weak secrecy; there are also other notions which are used to describe different secrecy levels such as ideal secrecy, semantic secrecy, and distinguishing secrecy.

Table 2.1 briefly explains and summarizes the conceptual meaning as well as the mathematical definition of the most popularly used secrecy notions in the literature. In the table, $I(\ ;\ )$ means the mutual information, K is the secret key sequence, pm is the probability distribution of the message; m, m' are defined to be different input messages and $\mathbb{V}(p_{\mathsf{X}}, p_{\mathsf{Y}})$ is the statistical or variational distance, which can be given as

$$\mathbb{V}(p_{\mathsf{X}}, p_{\mathsf{Y}}) \triangleq \int_{\mathbb{R}^n} |p_{\mathsf{X}}(\mathbf{x}) - p_{\mathsf{Y}}(\mathbf{x})| d\mathbf{x}. \tag{2.1}$$

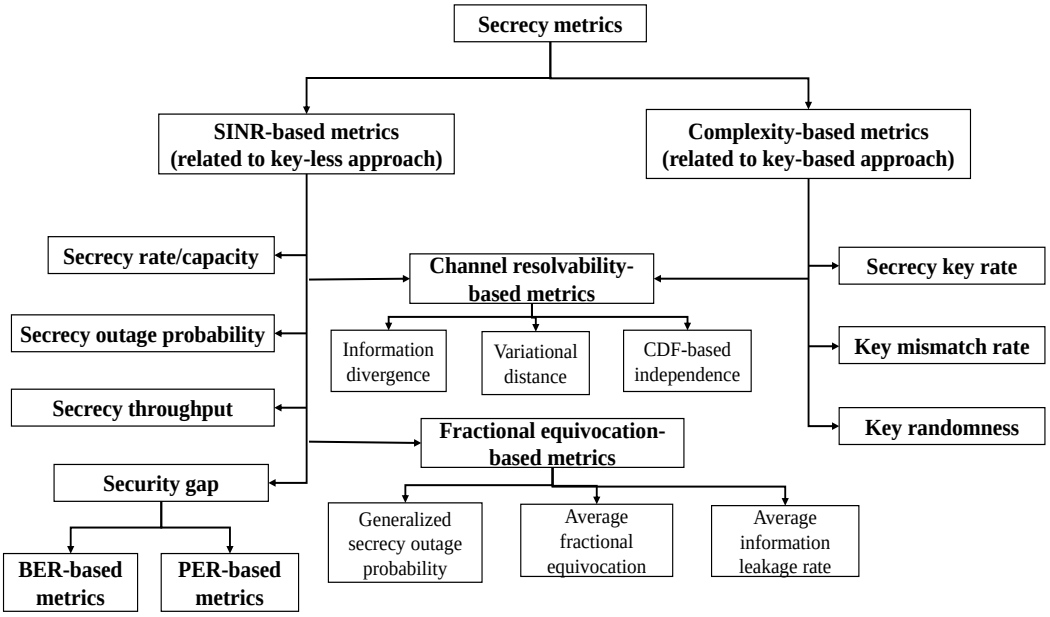


Figure 2.2: Classification of the common secrecy performance metrics used to evaluate the security performance of wireless schemes and techniques.

2.3.2 Secrecy Performance Metrics

One of the most important steps that has to be performed after designing any security scheme or technique is to properly evaluate and quantify its secrecy performance using a suitable metric. The performance evaluation must reflect how much secrecy the proposed scheme or method can provide. Without loss of generality, the secrecy metrics used in the literature can be classified into two major classes as exhibited in Fig. 2.2. The first class, which is associated with key-less-based PLS techniques, is named as SINR-based metric; whereas the second class, which is associated with key-based PLS methods, is called complexity-based metric.

The SINR-based metrics include secrecy rate or secrecy capacity, secrecy outage probability, secrecy throughput, fractional-equivocation-based metrics, BER-based and PER-based metrics. Secrecy channel capacity [4] is the most commonly used metric defined as the difference between the legitimate and eavesdropper's

channel capacities. More precisely, it defines the maximum secrecy rate at which the message is recovered reliably at Bob while keeping it useless and unrecoverable at Eve. This metric is later extended by researchers to outage secrecy and outage secrecy rate probability [31] in order to better measure the resulting secrecy in fading environments. Although secrecy capacity metric is very popularly used in the literature by information theoreticians, it does not necessarily reflect the actual obtained secrecy in practical transceiver designs with different communication services, but rather shows the achievable bounds considering the random channel behavior. However, to get the actual practical secrecy performance, error probability rate difference between Eve and Bob has been adopted by the signal processing and system design communities. An example on this is bit error rate (BER) [32] and packet error rate (PER) [33], which can directly be linked with secure throughput [34] and thus with secrecy channel capacity.

Despite the usefulness of traditional secrecy outage probability in evaluating and characterizing the security performance of wireless channels, it has three main demerits. First, it lacks the ability to quantitatively characterize the amount of information leakage to the eavesdroppers when outage secrecy happens. Second, it cannot provide any insights on the eavesdropper's capability in successfully decoding the confidential messages. Third, it cannot be linked with the Quality of Service (QoS) requirements of different applications and services. Motivated by these facts, authors in [35] proposed three new metrics based on the distribution of fractional equivocation (partial secrecy) given by ($\Delta = \frac{H(M|R_E)}{H(M)}$) [36], which can be obtained from channel gains distributions. These metrics include generalized secrecy outage probability, average information leakage rate, and average fractional equivocation.

The second class of metrics (i.e., complexity-based metric), is mainly used for key-based methods. This metric is adopted for this kind of methods because an eavesdropper may become eventually able to guess the key (if it has sufficient time and powerful processing capabilities) using exhaustive search process or what is commonly called as brute-force attack. In this approach [24], designers are mostly interested in measuring the length of the key extracted from the channel since the longer the key is the better the secrecy level will be as it would be harder for Eve

to crack the key. Note that keys are desired to be long enough with high entropy and uniform distribution. Besides, the key disagreement (mismatch) probability between the transmitter and receiver is a very important metric to be measured as it reflects whether the proposed method will degrade the legitimate receiver performance or not.

One important point we should emphasize here is that error rate probability at eavesdroppers does not fulfill any of the secrecy requirements in this case, thus it is not suitable to be used in key-based approach. Moreover, channel resolvability-based metrics [37] including information divergence, variational distance, and CDF-based independence between the transmitted message and its observation at Eve can be used to measure the secrecy of key-based methods as well as key-less methods. For more details on learning how to accurately measure and calculate these metrics alongside their mathematical definitions and the differences between them, we refer the readers to our recently published paper in [38].

2.4 Security Techniques Classifications

In Fig. 2.3 and Fig. 2.4, we explicitly draw and show from a high level perspective the big picture of PLS, the conceptual classification structure of PLS approaches divided into SINR-based and complexity-based ones. For each approach, we mention the kernel enabling techniques along with the main domains corresponding to each security technique including time, frequency and space. In this section, we classify and summarize the general enabling techniques one by one, explain their concepts, advantages, disadvantages, give examples from the literature on each technique, and finish each subsection with stating the lessons learned (taken notes) from each domain.

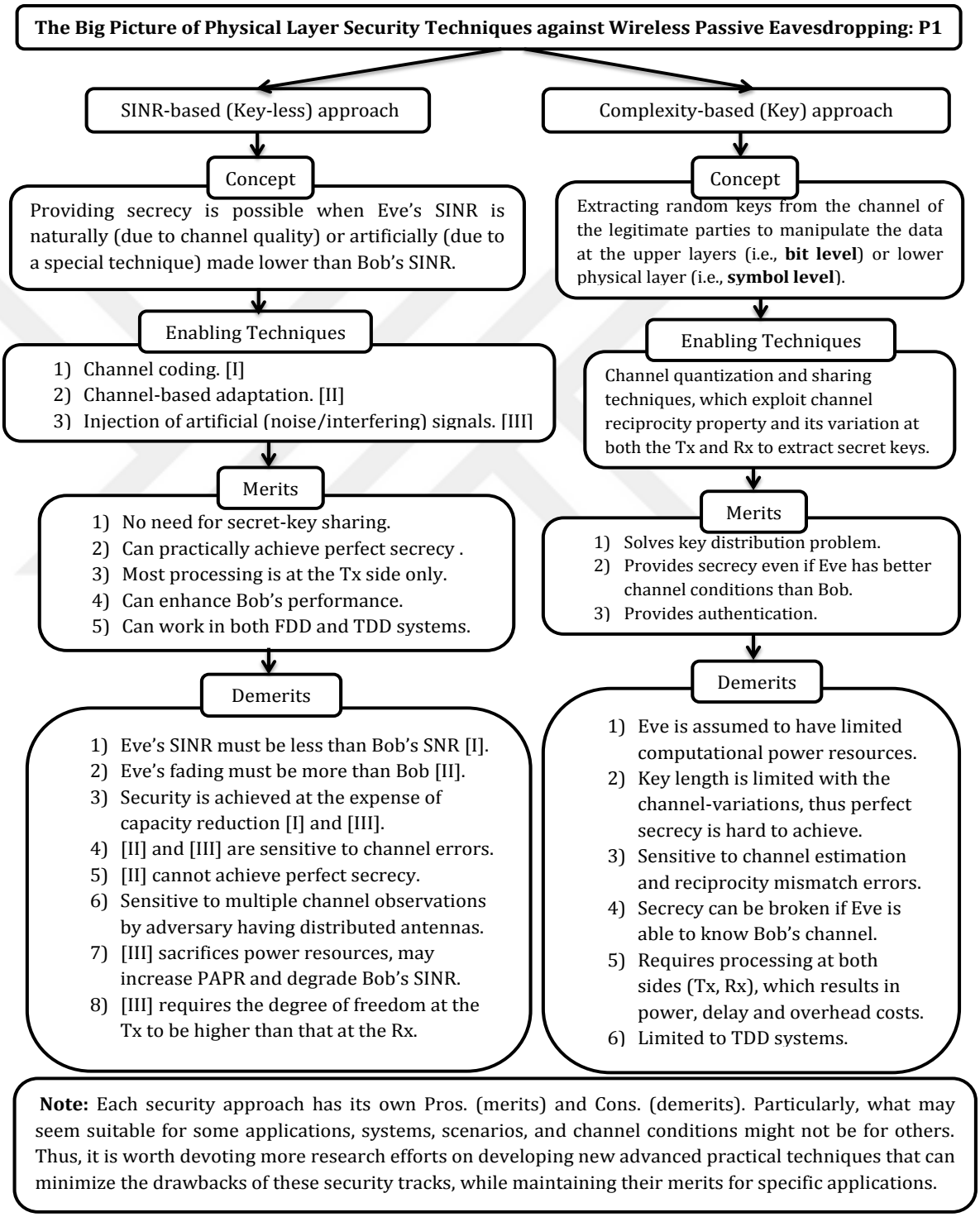


Figure 2.3: The big picture of the classification structure (including concepts, merits, and demerits) of physical layer security techniques against wireless passive eavesdropping: Part one (P1).

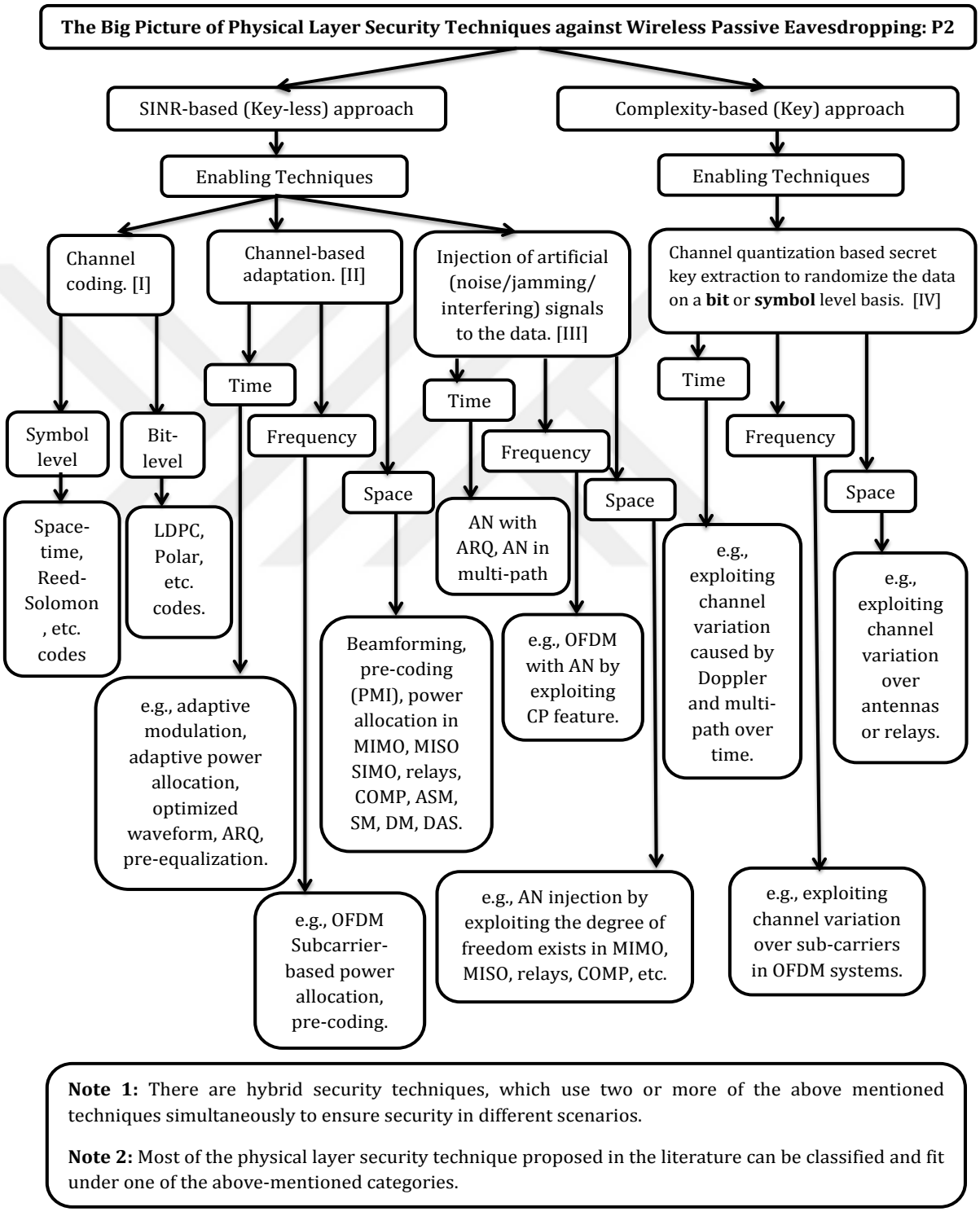


Figure 2.4: The big picture of the classification structure (including examples in the three main signal domains: time, frequency, and space) of physical layer security techniques against wireless passive eavesdropping: Part two (P2).

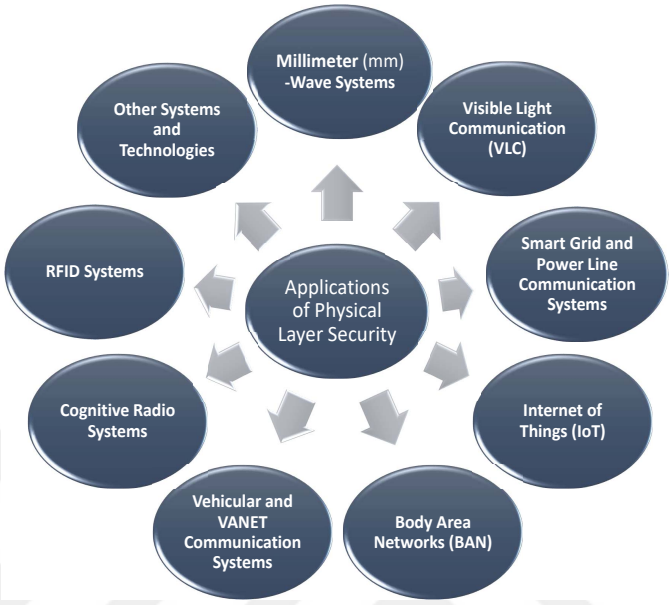


Figure 2.5: Main applications of physical layer security to different systems and technologies.

2.5 Applications of Physical Layer Security

In spite of the fact that many research efforts have been conducted to analyze, characterize, investigate and develop new PLS techniques, most of these works have merely been concentrated on traditional and classical wireless scenarios. However, due to the special characteristics, requirements and features of many other important, emerging communication technologies and systems, new efforts and studies have started accounting and considering PLS for these special systems, such as VLC, smart grid, PLC, IoT, BAN, RFID, vehicular Ad-hoc, cognitive radio, UAV, UWB, D2D, RFID, index modulation, NOMA and mm-Wave technologies. In this section, we present a comprehensive review of the state of the art on applying PLS to these new types of communication scenarios. It should be emphasized that there are generally three main factors that affect the adoption of PLS in any communication technology. These factors can be summarized as below: 1) the channel characteristics of the considered system or scenario, 2) the capabilities and structure of the transceiver design, and 3) the system requirements needed to meet a certain satisfactory performance level for a specific service or application.

Secrecy Notions	Conceptual Definition	Mathematical Definition
Perfect secrecy	The mutual information leakage to Eve must be zero regardless of its processing power and computational capabilities. This notion serves as the most stringent secrecy measure as it ensures almost unity decoding error probability if the entropy of the message is the same as that of the key.	$I(M;R_E)=0,$ $H(M)=H(M \mid R_E).$
Ideal secrecy	The asymptotic conditional entropy of the both the message and the key does not go to zero as the codeword length n goes to infinity. This means that an encryption algorithm is ideally secure if no matter how much of cipher text is intercepted by Eve, there is no unique solution of the plaintext but many solutions of comparable probability.	$\lim_{n\to\infty} H(M \mid R_E) \neq 0,$ $\lim_{n\to\infty} H(K \mid R_E) \neq 0.$
Weak secrecy	The asymptotic mutual information rate goes to zero as the codeword length n goes to infinity. Thus, this notion does not strictly force mutual information leakage to be zero on each channel use, but rather on average.	$\lim_{n\to\infty} \frac{1}{n} I(M;R_E) = 0\,.$
Strong secrecy	The asymptotic mutual information goes to zero as the codeword length n goes to infinity. Thus, this notion forces mutual information leakage to be zero on each channel use, but not on average as in weak secrecy	$\lim_{n\to\infty} I(M;R_E) = 0.$
Semantic secrecy	It means that it is asymptotically impossible to estimate any function of the message better than to randomly guess it without knowing or considering Eve's observations and over all message distributions.	$\lim_{n\to\infty} \max_{pm} I(M;R_E) = 0.$
Distinguishing secrecy	It means that the channel output observations are asymptotically indistinguishable for different input information messages. This achieves strong secrecy over all message distributions.	$\lim_{n\to\infty} \max_{m,m'} \mathbb{V}(p_{R_E\mid M=m}, p_{R_E\mid M=m'}) = 0,$ $\mathbb{V}(p_{\mathrm{X}}, p_{\mathrm{Y}}) \triangleq \int_{\mathbb{R}^n} (\mid p_{\mathrm{X}}(\mathbf{x}) - p_{\mathrm{Y}}(\mathbf{x}) \mid) d\mathbf{x}.$

Table 2.1: Secrecy notions: meaning and mathematical definition.

Chapter 3

Joint PHY/MAC Layer Security Design Using ARQ with Adaptive Modulation and Null-Space Independent, PAPR-Aware Artificial Noise

3.1 Introduction

To mitigate the effect of the problems and issues associated with classical cryptography, key-less information-theoretic-based schemes have attracted the research community's attention due to their desirable features. In Wyner's paper [4], it was stated that confidential communication between legitimate users is possible without secret key sharing if the channel of the eavesdropper (Eve) is worse than the channel of the intended receiver (Bob). Motivated by the same study [4], the achievable secrecy capacity from an information-theoretic point of view was studied for various communication scenarios and channels, which were surveyed in [6,8,39]. In particular, information-theoretic secrecy under channel coding and

automatic-repeat-request (ARQ) was studied for the case where Eve's signal-to-noise ratio (SNR) is lower than that of Bob in [40–44].

However, in practical scenarios, due to the random, location-dependent, and broadcast nature of the wireless channel; Eve's channel condition including its received SNR can be comparable to or even better than Bob's one [45]. Therefore, well-advanced and practical security techniques are extremely needed to ensure the secrecy for legitimate users. In the literature, various PHY security methods have been proposed and comprehensively surveyed in [6], [8], and [39]. To the best of our knowledge, most of these methods mainly depend on exploiting one or more of the following approaches: 1) the channel variations and its reciprocity with the assistance of diversity to extract shared secret keys [46], [47]; 2) space diversity such as MIMO, relays, and large scale networks to, for instance: inject artificial noise (AN) [48], perform precoding, shape antenna patterns (beam-forming) towards trusted users [27], etc.; 3) specific features in certain systems such as cyclic prefix, pilots, hardware impairments, and synchronization to disrupt Eve's reception [49–53]. However, when these degrees of freedom are not available, PHY security becomes extremely hard to achieve. Despite of all these constraints, security can still be provided by exploiting some already existing features in MAC layer, which are linked with the quality of service (QoS) requirements. For instance, employing (ARQ/HARQ) protocol, that takes an advantage of the fact that only intended recipients can request retransmissions, can be used to enhance security [54]. In [55], authors studied the optimal power allocation sequence over the HARQ rounds that maximizes the outage probability of Eve, without considering the effect of the transmission parameters. They assumed that the statistical knowledge of Eve's channel and SNR levels are available at the transmitter. However, such an assumption might be impractical since Eve is usually a passive receiver in reality [6], [56]. Additionally, they considered that the channel exhibits quasi-static fading, which is not necessarily the case in many practical scenarios [57], [58]. Without relying on the aforementioned assumptions, we investigated and quantified in [33] the exact practical secrecy gap between Bob and Eve due to adopting a special design of ARQ. It is shown that although ARQ scheme can provide secrecy, it fails to deliver enough of it at high SNR values or when Eve's SNR is higher than that of Bob, making Eve able to decode the

packet correctly from the first round [33]. To mitigate this problem, we proposed adaptive modulation to enhance the obtained secrecy. However, the enhancement was not sufficient enough and not applicable over all SNRs [33].

Moreover, we propose a new joint PHY/MAC layer security method that exploits ARQ with maximal ratio combining (MRC) process alongside a special design of AN to provide secrecy even if Eve's SNR is higher than that of Bob. Under realistic assumptions, it is shown that the information-theoretic perfect secrecy notion[1] can practically be achieved by the proposed method. Furthermore, the method preserves its applicability for the worst security scenario, where the legitimate channel is flat (not providing much randomness) and the transmitter is equipped with only a single antenna. On the other hand, it is also noticed that perfect secrecy is not always needed to provide a perfectly secure service. In reality, each service has different QoS requirements than the others, and if we ensure that Eve is operating below these requirements, then practical secrecy can be guaranteed. **The main contributions** of this paper can be summarized as follows:

- The exact secure throughput, resulting from the implicit adaptivity, caused by using ARQ scheme with MRC employed on a symbol level basis, is determined and quantified by analysis and simulations, and then used as a benchmark for comparison purposes with the performance of the new proposed designs.

- ARQ with QoS-based adaptive modulation is introduced as a mechanism to provide QoS-based secrecy.

- A new security method based on ARQ mechanism with null-space-independent AN that exploits the receiver structure of MRC is developed to ensure security for various data services such as voice and video. Thus, instead of relying on the null-space created by the degree of freedom that exists in the case of multiple antennas [48], [27], cooperative relays [59], frequency-selective channel [49], or cyclic prefix feature in OFDM [50], for

[1]Perfect secrecy means that the mutual information leakage to Eve is equal to zero (i.e., the decoding error probability of Eve must go to unity).

AN generation; in this work, ARQ with MRC is exploited for the first time in the literature for producing null-space-independent AN to safeguard transmission against eavesdropping attacks. Basically, AN is designed based on the quality of service (QoS) requirements and the channel condition between the legitimate parties and injected to the data packet. If the same packet is requested by Bob, an AN canceling signal is designed based on the legitimate user's channel and added to the next packet. Then, an AN free packet is obtained by using MRC process, whereas the AN severely deteriorates the eavesdropper's performance.

- Closed form expressions of the achievable secure throughput for voice and video services are derived, which can be used by designers to quantify the secrecy performance of the proposed design.

- Two important security-related problems are addressed: 1) the combined practical design of secrecy, reliability, throughput, delay, and the trade-off among them; 2) the peak-to-average power (PAPR) increase, resulting from the structure of the added AN.

- The scheme is extended to multi-carrier systems (OFDM) over a frequency selective channel to demonstrate how a designer can exploit and optimize the added AN to not only improve secrecy, but also to reduce the PAPR and out-of-band emission (OOBE) in OFDM systems.

The merits of the proposed scheme can be stated as follows:

- It is structurally simple but very effective, and it does not require to be supported by a complicated transceiver architecture. More importantly, it does not require any changes or extra processing at the receiver side thanks to the proper design of the added AN, which can be perfectly canceled during the MRC process.

- It can provide prefect secrecy with the aid of the added AN. This ensures zero information leakage to Eve even if Eve's SNR is higher than Bob's one.

- It can provide secrecy in one of the most challenging scenario, where there is no spatial degree of freedom (no null-space) and the channel is flat fading (i.e., no much randomness).

- The proposed design creates an extra degree of freedom in the power domain due to the added AN, which can be utilized not only to enhance secrecy, but also for other purposes alongside secrecy such as reducing PAPR and mitigating OOBE of OFDM-based systems. In other words, the scheme increases the system design flexibility.

- It can serve as an alternative solution for the jamming-aided eavesdropping problem presented in [60]. In this problem, Eve jams Bob to force him to ask for retransmission so that she can get more copies of the same packet, and thus increasing her decoding capability. However, since in our scheme AN is added to each retransmission round, this will prohibit Eve benefiting from the retransmitted copies of the same packet. Interested readers can refer to [60] for more details.

- The maximum benefit and best operating condition of the proposed scheme can be obtained when it is used with OFDM-based waveforms over dispersive channels. This is due to two reasons: 1) the AN vector's randomness becomes not only a function of the generated signal at the source, but also of the dispersive channel randomness; 2) the possibility of redesigning the AN to solve some of the major drawbacks of OFDM, as it will be shown in Section V.

The remainder of this chapter is ordered as follows: Section 3.2 gives the details of the system model and the main adopted assumptions. Section 3.3 provides the description and explanation of the proposed ARQ with adaptive AN security scheme. The analytical analysis of the achievable secure throughput is presented in Section 3.4. Section 3.5 explains ARQ with adaptive modulation transmission for providing QoS-based secrecy. The extension of the proposed scheme to OFDM is explained in Section 3.6, where two new optimization problems related to PAPR and OOBE are formulated and solved numerically. Section 3.7 exhibits and discusses the simulation results of the developed method. Finally, conclusion

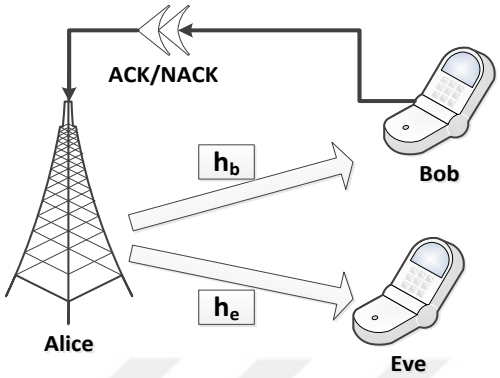


Figure 3.1: Concise and simple model of the considered security scenario.

and future works are drafted in Section 3.8.

Notations: Vectors are denoted by bold-small letters, whereas matrices are denoted by bold-large letters. Norm-2 and norm-infinity are defined by $\|\cdot\|_2$ and $\|\cdot\|_\infty$, respectively. $\mathbf{I}_N$ is the $N \times N$ identity matrix. The transpose, conjugate transpose, inverse, and absolute value (amplitude) are symbolized by $(\cdot)^T$, $(\cdot)^H$, $(\cdot)^{-1}$, and $|\cdot|$, respectively.

3.2 System Model and Preliminaries

We consider a single-input single-output (SISO) communication system employing ARQ protocol as briefly presented in Fig. 3.1. In particular, a source node (Alice) is communicating with a legitimate user (Bob) in the presence of a passive eavesdropper (Eve), who tries to intercept the source information of a service, communicated between the legitimate parties (Alice and Bob). The transmission mechanism of ARQ without AN, as shown in the lower part of Fig. 3.2 and before connecting the adaptive artificial noise (AAN) block, works as follows. First, Alice encodes the information bits using cyclic redundancy check (CRC), maps the bits into symbols using M-ary phase shift keying (M-PSK) and then forms a data packet $\mathbf{x} = [x_1\, x_2 \cdots x_N]^T \in \mathbb{C}^{N\times 1}$ of N number of modulated symbols, to be sent to Bob. After receiving the transmitted packet, which passes through a Rayleigh

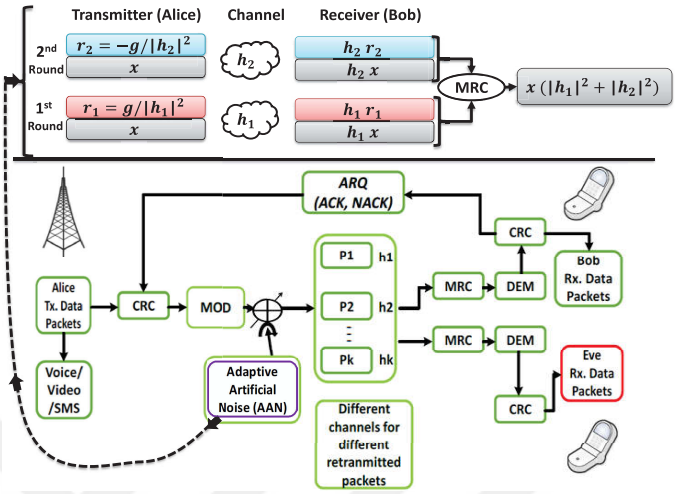


Figure 3.2: The detailed system model of the proposed security scheme.

fading channel and affected by additive white Gaussian noise (AWGN), Bob demodulates and then decodes the packet using CRC. Based on the decoding result of the CRC, Bob decides success or failure of packet decoding by sending back to Alice an ACK or NACK messages through an error-less feedback channel, which is accessible by Eve as well. If a NACK is received by Alice and the current retransmission value is less than the maximum number of allowable retransmissions (L), Alice resends the same data packet with identical transmission parameters to the first round, i.e., same power and modulation during each retransmission. The receiver then uses MRC on a symbol level basis (before demodulation process) to combine the last received data packet with the previously erroneous received ones, which are stored in a buffer (i.e., soft-combing is used). If ACK is received by Alice or L is reached, Alice stops retransmitting the current same packet and instead transmits a new data packet. In each retransmission round, both Bob and Eve try to detect the transmitted packet by combining the received data from all preceding retransmissions of the same packet via MRC. If Bob cannot extract the packet after L rounds, then Bob records a packet error. This transmission mechanism is referred to in the literature (e.g., [58], [61]) as chase combining ARQ (CC-ARQ) scheme. Note that adaptive artificial noise (AAN) block is initially excluded from the system and the explanation of this block is left for the next section.

The following assumptions are also adopted: 1) Both channels, Alice-to-Bob

(h_b) and Alice-to-Eve (h_e) are considered to be independent and identically distributed (i.i.d.) block Rayleigh fading with constant gain over each ARQ round, but independent across ARQ rounds [57], [58], [61]. 2) A maximum of L ARQ rounds is allowed which limits both complexity and delay. 3) Alice has no knowledge on Eve's channel since Eve is a passive node. 4) Alice has the normal feedback information about Bob such as ACK/NACK signals [33]. Also, in the case of ARQ with AN scheme, Alice has knowledge on h_b, but not h_e [58]. 5) The channel reciprocity property is adopted, where the downlink channel can be estimated from that of the uplink in a time division duplexing (TDD) system. Thus, Eve does not know the channel of the legitimate link [62]. 6) The worst (most difficult) security scenario is considered, where the channel is not providing much randomness (one tap channel) and Eve is aware of the retransmission process by accessing the feedback messages and also uses MRC (optimal receiver structure) similar to Bob [33]. 7) Each one of the communicating parties (Alice and Bob) is equipped with a single antenna as well as Eve [55]. 8) Both Bob and Eve experience independent channel realizations because the wireless channel response is dependent on the positions of the communicating parties as well as the environment [56], [49].

3.3 ARQ with Adaptive Artificial Noise

Here, we divide our work into two parts: the first is dedicated to studying and investigating CC-ARQ scheme before adding AN as explained in Section II, which will be used as a benchmark for comparison purposes; while the second is devoted to developing a new security method based on ARQ with MRC and AN. For the first part, as explained earlier, Alice transmits data packet $\mathbf{x}$ with average power at the k^{th} round denoted by P_k. The received signal vectors, whose sizes are the same as $\mathbf{x} \in \mathbb{C}^{N\times 1}$, at both Bob and Eve in the k^{th} round are modeled as

$$\mathbf{y}_{i,k} \;=\; h_{i,k}\mathbf{x} + \mathbf{w}_{i,k}, \quad k = 1, 2, \cdots L, \;\; i \in \{b, e\}\,, \tag{3.1}$$

where the subscripts b and e indicate the parameters for Bob and Eve. Thus, when $i = b$ and $i = e$, we will have $h_{b,k}$ and $h_{e,k}$, which are the block-fading Rayleigh

channel realizations of Alice-to-Bob and Alice-to-Eve links over the k^{th} round, respectively; whereas $\mathbf{w}_{b,k}$ and $\mathbf{w}_{e,k}$ are the complex additive white Gaussian noise vectors with power spectral density of $N_{b,k}$ and $N_{e,k}$ at Bob and Eve, respectively. Additionally, we define $\gamma_{i,k}$ and $\bar{\gamma}_{i,k}$ to be the instantaneous and average received SNR of both Bob and Eve at k^{th} round, which are given by $\gamma_{i,k} = \frac{P_k|h_{i,k}|^2}{N_{i,k}}$ and $\bar{\gamma}_{i,k} = \frac{P_k}{N_{i,k}}$, respectively. As mentioned before, in this scheme, MRC is performed on a symbol level basis before demodulation, where each version of the received signal at each round is multiplied by the corresponding channel realization conjugate ($*$) and thus the net combined received signal at Bob/Eve after L rounds can be expressed as

$$\hat{\mathbf{y}}_i = \sum_{k=1}^{L} \mathbf{y}_{i,k} \times h_{i,k}^* \tag{3.2}$$

$$= \sum_{k=1}^{L} (h_{i,k}\mathbf{x} + \mathbf{w}_{i,k}) \times h_{i,k}^* \tag{3.3}$$

$$= \sum_{k=1}^{L} |h_{i,k}|^2\mathbf{x} + \mathbf{w}_{i,k}h_{i,k}^*. \tag{3.4}$$

For the case of voice service, where $L = 2$, the above formula can be reduced to the below form

$$\hat{\mathbf{y}}_i = \mathbf{y}_{i,1}h_{i,1}^* + \mathbf{y}_{i,2}h_{i,2}^* \tag{3.5}$$

$$\hat{\mathbf{y}}_i = \mathbf{x}\left(|h_{i,1}|^2 + |h_{i,2}|^2\right) + \hat{\mathbf{w}}_i, \tag{3.6}$$

where $\hat{\mathbf{w}}_i = \mathbf{w}_{i,1}h_{i,1}^* + \mathbf{w}_{i,2}h_{i,2}^*$, and the detected data packet $\hat{\mathbf{x}}$ is given as

$$\hat{\mathbf{x}} = \mathbf{x} + \frac{\hat{\mathbf{w}}_i}{(|h_{i,1}|^2 + |h_{i,2}|^2)}. \tag{3.7}$$

Now, since Bob's channel is independent of Eve's one, the implicit adaptation process resulting from ARQ mechanism and controlled by Bob will be in favor of him, but not Eve because the retransmission happens according to Bob's channel condition, but not Eve's one. In other words, there are cases where Eve requires two rounds to be able to decode due to her possible bad channel conditions, but Bob may require only one round to decode as he may have a good channel gain in the first round. Since Bob controls the retransmission process, a second retransmission, which may be needed for Eve to decode, will not be triggered as Bob

is able to decode successfully from the first round. Consequently, Eve's packet error rate (PER) will be significantly affected not only by the channel conditions but also by the number of occurred retransmission. Simulation results exhibit that the use of ARQ in the described way can provide a significant PER secrecy gap between Bob and Eve and thus secure throughput at a specific SNR region, which will be accurately identified in the forthcoming sections.

However, CC-ARQ scheme alone, as described before, is not sufficient to provide eavesdropping-resilient services at any SNR Eve may have. In fact, insecure transmission occurs in two cases. The first case happens when Eve is closer to the transmitter than Bob, in this situation, Eve will be able to decode the packet from the first round due to experiencing high average SNR, resulting in zero secrecy gap [38], [52]. Thus, with respect to Eve, there is no need for extra retransmissions. The second case occurs when both Bob and Eve have a very high signal quality, thus, both of them will be able to decode the packet successfully from the first round. Consequently, the adaptivity process, which was in favor of Bob and giving him better performance than Eve is no longer applicable. These two intuitive factual issues, which are verified by our performed results as it will be shown later, substantiate the key motivation for the next proposed design.

To overcome the problem of insecure transmission in the aforementioned scenarios, especially for those cases where perfect secrecy is required over all expected SNRs, we propose a new, simple, practical and very effective security scheme, by which ARQ along with MRC is exploited for the first time in the literature for generating null-space independent artificial noise that can be automatically canceled at only the legitimate user without any extra processing. Particularly, an interfering signal (i.e, AN) based on the channel gain and QoS requirements of the legitimate user, is added on top (in the power domain) of the transmitted data signal $\mathbf{x}$ in each retransmitted round as shown in the upper part of Fig. 3.2. The added interfering AN signals[2] are designed in such a way that when

[2]For services other than voice, i.e., for the case of $L > 2$, we perform AN addition as follows. We first check whether L is odd or even, if it is even, we add AN with each retransmission round based on the corresponding channel responses, but if it is odd, then two design options can be used. Option I: we leave the last retransmission round without adding AN so that a balance in the added AN can be achieved and then AN can be canceled without changing the receiver structure. Option II: we add to the last retransmission round the opposite of the added AN in

they get combined at the receiver side using MRC process, they will compensate each other at the Bob's side only, while Eve will suffer a severely degraded performance. To achieve this, the designed AN, which does not depend on having null-space in the channel as opposed to the existing AN-based security schemes in the literature (e.g., [48], [50]), is properly added on top (power domain) of the time[3]domain signal vector to the first and second retransmission rounds, making the newly received signal vectors in the first and second rounds appear as

$$\mathbf{y}_{i,1} = h_{i,1}\left(\mathbf{x}+\mathbf{r}_1\right)+\mathbf{w}_{i,1} \tag{3.8}$$

$$\mathbf{y}_{i,2} = h_{i,2}\left(\mathbf{x}+\mathbf{r}_2\right)+\mathbf{w}_{i,2}, \tag{3.9}$$

where $\mathbf{r}_1 \in \mathbb{C}^{N\times 1}$ and $\mathbf{r}_2 \in \mathbb{C}^{N\times 1}$ are the added AN vectors to the first and second rounds, respectively. After MRC at the receiver side, $\hat{\mathbf{y}}_i$ becomes

$$\hat{\mathbf{y}}_i = \mathbf{y}_{i,1}h_{i,1}^* + \mathbf{y}_{i,2}h_{i,2}^* \tag{3.10}$$

$$\begin{aligned}\hat{\mathbf{y}}_i &= \mathbf{x}\left(|h_{i,1}|^2+|h_{i,2}|^2\right)\\ &+ \mathbf{r}_1|h_{i,1}|^2+\mathbf{r}_2|h_{i,2}|^2+\hat{\mathbf{w}}_i.\end{aligned} \tag{3.11}$$

From (11), we find that it is possible to design $\mathbf{r}_1$ and $\mathbf{r}_2$ at the transmitter in such a way that ensures full cancellation of the added AN at only Bob as graphically depicted in the upper part of Fig. 3.2. To achieve this, $\mathbf{r}_1$ and $\mathbf{r}_2$ are designed to be a function of the legitimate user's channel power ($|h_{b,k}|^2$) and a random AN vector $\mathbf{g}$ as follows:

$$\mathbf{r}_1 = \frac{\mathbf{g}}{|h_{b,1}|^2} \quad , \quad \mathbf{r}_2 = \frac{-\mathbf{g}}{|h_{b,2}|^2} \tag{3.12}$$

$$\mathbf{g} = \sqrt{\frac{\varphi}{2}}\left((2\mathbf{u}-1)+j(2\mathbf{q}-1)\right) , \tag{3.13}$$

the first round; however, the legitimate receiver structure needs some modification in this case to properly cancel the added AN. Specifically, the second received round has to be combined with the first one using MRC and saved in buffer I, then the third received round has to also be combined with the first one using MRC and saved in buffer II. Finally, the content of buffer I can be added to that of buffer II in order to get an AN-free packet at the legitimate receiver. In this paper, we adopt using option I as it does not require receiver structure modification and can serve as the worst security scenario for the proposed scheme.

[3]It is important to note here that in a **multicarrier** system with multitap (frequency selective) channel, the AN signal will be added on top of the **frequency** domain of the transmitted signal. In this case, the received vector signals at both Bob and Eve in the k^{th} round can be modeled as $\mathbf{y}_{i,k} = \mathbf{H}_{i,k}\left(\mathbf{x}+\mathbf{r}_k\right)+\mathbf{w}_{i,k}$, where $\mathbf{H}_{i,k} \in \mathbb{C}^{N\times N}$ is the diagonal frequency response matrix of a multitap channel. The added AN signals will cancel each others at only Bob by using MRC in the frequency domain.

where $\mathbf{g} = [g_1\ g_2\ \cdots\ g_N]^T \in \mathbb{C}^{N\times 1}$ can be seen as an AN vector, whose samples change independently from one symbol to another according to a certain distribution. Therefore, $\mathbf{g}$ can also be perceived as a one-time pad key [63], whose length is equal to the message length with entropy equals to that of the message, and does not require to be shared with the receiver. It should be emphasized that although the AN vector in our scheme is perceived to be similar to one-time pad key in the sense that it can achieve perfect secrecy notion as described by Shannon with zero information leakage to Eve; it is however fundamentally different in the sense that the key (i.e., AN in our case) is not known to the receiver. It is also worth mentioning that the design of $\mathbf{g}$ gives freedom in: 1) modifying the structure (or distribution) of the added AN; 2) adjusting the power of the added AN, which is done based on the QoS requirements; and 3) controlling the PAPR problem resulting from the added AN by designing it to have a constant envelope with a uniform phase distribution. In the proposed scheme, $\mathbf{g}$ is deliberately designed to have a *uniform* phase distribution with a constant envelope (like a QAM signal) as in (13), in which φ is the power (variance) of the added AN vector and it is optimized based on the QoS requirements as well as the targeted security level as it will be shown later. Without loss of generality, $\mathbf{g}$ is properly designed so that PAPR problem can be avoided as uniform phase distribution has a constant envelope, resulting in a zero increase in the PAPR. To achieve this, the samples of $\mathbf{u}$ and $\mathbf{q}$ vectors are chosen to be Bernoulli-distributed random variables with values of ones and zeros. It should also be emphasized that most of the AN-based security methods existing in the literature are merely using Gaussian distributed noise, which leads to a significant increase in the PAPR as it does not have a constant envelope. To the best of our knowledge, PAPR problem has generally been ignored in the existing AN-based security methods, while this work sheds the light on this problem and proposes a practical solution to address this issue.

Fig. 3.3 is drawn to show the huge difference in the baseband PAPR between the conventional Gaussian distributed AN and the proposed uniformly distributed AN. It is evident from Fig. 3.3 that the proposed one, colored by a blue line, has a constant unity PAPR, while the PAPR of the conventional one is ranging from 6 dB to 12 dB (very high values causing power amplifier problems). Note

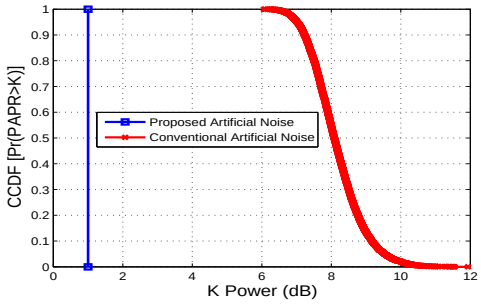


Figure 3.3: Baseband peak-to-average power ratio (PAPR) comparison between the conventional AN-based methods with Gaussian distribution and our proposed AN design with uniform distribution.

that the proposed AN design has unity PAPR because oversampling and pulse shaping are not included in our design. However, the PAPR of a QPSK signal in passband (when up-sampling with pulse shaping is considered) will not be unity, but rather twice that of the baseband PAPR. It should also be mentioned that Fig. 3.3 shows only the PAPR of the added AN signal instead of the PAPR of the combination of the added AN signal and the original signal. The reason for that is the fact that adding the proposed AN signal to an M-PSK modulated signal of a constant amplitude will not affect the PAPR of the combined signal. However, in Section V, we will consider the PAPR of the combined signal because the AN vector there will be added to an OFDM signal of variable amplitude (not M-PSK signal of constant amplitude).

Aside from PAPR, having uniform distribution is more desirable from a security perspective than Gaussian, because it has larger variance and creates complete randomness as well as full uncertainty in the added AN samples. Particularly, each sample value in $\mathbf{g}$ has equal probability and thus very high entropy, which is the same as the property of good secret keys [64].

At the receiving sides, the detected data signal vectors at both Bob and Eve become, respectively, as follows:

$$\hat{\mathbf{x}}_b = \mathbf{x} + \frac{\hat{\mathbf{w}}_b}{(|h_{b,1}|^2 + |h_{b,2}|^2)} \tag{3.14}$$

$$\hat{\mathbf{x}}_e = \mathbf{x} + \frac{\hat{\mathbf{w}}_e + \mathbf{r}_1|h_{e,1}|^2 + \mathbf{r}_2|h_{e,2}|^2}{(|h_{e,1}|^2 + |h_{e,2}|^2)}. \tag{3.15}$$

It should be clear that when the values of $\mathbf{r}_1$ and $\mathbf{r}_2$ are substituted in (11),

the intentionally added AN gets totally canceled. Thus, the detected $\hat{\mathbf{x}}$ packet shown in (14) is the same as that in (4). This means that Bob's packet error rate (PER) performance will not be affected after employing this method whatsoever. Looking back at Eve's side, one can infer that since Eve neither knows the channel of Alice (due to using sounding techniques to estimate the channel in TDD systems) nor the added AN vector $\mathbf{g}$ (due to not sharing it with any communication party), a considerable degradation will occur whether Eve is using MRC or not. If she employs MRC, then an additional interfering noise resulting from non-zero subtraction process will affect her PER. On the other hand, if she does not employ MRC, then the AN added to each retransmission round will automatically affect her PER. It should be stated that the secrecy is enhanced by the proposed scheme because of 1) the added AN vector $\mathbf{g}$, and 2) the asymmetric CSI availability and the independence of channel states between Bob and Eve from one side and between different rounds from another side. Moreover, an additional source of secrecy can be obtained when the channel is not flat fading, but rather dispersive in time, frequency, or both. The details and investigation of the scheme in dispersive channels is beyond the scope of this paper and left for future works.

Although this method provides a good practical security performance against Eve without affecting the reliability (i.e., PER) of Bob, it is observed that this performance is achieved at the expense of extra retransmission rounds, causing small delay and slight throughput reduction, which can be fully controlled according to the secrecy and QoS requirements. This reduction happens since the first round of each transmitted packet might be received in error even at high SNR due to the added AN. Thus, a second retransmission is usually needed to compensate the intentionally introduced error (uncertainty) in the first round. In fact, this throughput degradation problem occurs due to most Wyner's secrecy codes proposed in the literature [3]-[7]. On the other hand, it was mentioned in the latest state-of-the-art security survey paper [8] that the joint design of secrecy, reliability, and throughput with delay are challenging tasks to be studied and hopefully resolved in the future as the three factors are coupled and influencing each other. To the best of our knowledge and based on the surveys in [6], [8], and [39], such an issue has not been comprehensively investigated from a practical

perspective. Thus, besides the proposed design, this work also comes to put a step forward towards studying the mutual effect of these factors on each other, and to also find out the best trade-off that can ensure security without exceeding the QoS requirements determined by PER, delay, and throughput.

To mitigate the aforementioned throughput degradation's problem, we re-design the AN to be not only based on the channel of Bob but also on the QoS requirements of the requested service. Thus, adaptive AN (AAN) is added with just enough power to degrade Eve's reception, while trying to keep Bob's performance the same as it was before introducing the AN. The following steps summarize how to perform and employ the proposed security method in the context of LTE and future 5G and beyond networks:

1. The transmitter (Enode-B) determines which service the legitimate wireless user is intending to use.

2. According to the requested service, Enode-B (Alice) determines a PER threshold (PER_t) from a look-up table, as presented in Table 3.1, which is required to reliably accommodate a legitimate user with the requested service.

3. Based on the determined PER and from the extensive off-line PER simulation results obtained for Eve, Enode-B identifies the corresponding required SNR for Eve (SNR_t^e) to eavesdrop the service reliably. It should be noted that SNR_t^e is determined from the off-line simulation results, which are shown in Fig. 3.5 (a) and Fig. 3.6 (a). Particularly, we determine the value of SNR_t^e at which Eve's PER becomes less than PER_t, which is required to use a certain service reliably.

4. From the found SNR, Enode-B calculates a rough numerical value of the needed noise power to sufficiently degrade Eve's performance using this formula, $\varphi = 10^{\frac{-SNR_t^e(dB)+10}{10}}$.

5. A uniformly distributed noise with the previously calculated power, is intentionally added on top of the transmitted packet in the first and second

Table 3.1: QoS Lookup Table [1] with power (φ) of AAN required to achieve secrecy.

Service	Delay	L	PER_t	SNR_t^e	φ
Voice	100 ms	2	10^{-2}	30 dB	0.01
Video	150 ms	3	10^{-3}	40 dB	0.001

retransmission round in such a way that they will cancel each other after they get combined at only the intended receiver as explained before.

According to this method, it is noticed that in many daily used services such as voice and video, we do not actually need to have perfect secrecy to obtain a completely secure communication. That is because this method imposes Eve to operate in such a way that she is not able to achieve the QoS requirements necessary to intercept these services and use them reliably. Thus, there is no way to benefit from the undergoing service. Although we have targeted from the beginning to provide a good trade-off among reliability, throughput, delay and secrecy, our method shows that perfect secrecy can be achieved to provide fully secure messaging service at the expense of only half-throughput degradation. This is attained by making sure that the first packet transmission in the first round is always received in error, while the retransmitted packet in the second round can entirely cancel the noise added in the first round by sending an appropriate noise power. It is found by using extensive simulation that this can be achieved by making the variance of the added AN equal to the Bob's SNR value (i.e., $\varphi = SNR_{dB}$).

3.4 Analytical Analysis of the Achievable Secure Throughput

Finding exact formula for the achievable secure transmission efficiency or secure throughput ($S\eta$) under the proposed ARQ scheme with and without AN would

be useful and helpful to security designers in quantifying the exact achievable secrecy performance. In this work, $S\eta$ is determined by calculating the difference between Bob's throughput η^b and Eve's one η^e, where the throughput (η) itself is basically defined as the ratio of the number of information Packets Received Successfully (PRS) to the Total number of Transmitted Packets (TTP) including the retransmitted ones [57]. Thus, throughput (η) can be regarded as the complement of packet error rate (PER). The retransmitted packets are included in the throughput calculation in order to take the effect of the retransmission process on the average delay. Additionally, our analysis takes into consideration the implicit adaptivity process of ARQ along with MRC process. Also, practical discrete M-PSK signaling is considered in the analysis instead of the impractical Gaussian signaling in order to limit the peak transmission power and preserve low receiver complexity [50]. Given the aforementioned practical conditions, $S\eta$ can mathematically be defined as [38]

$$\begin{aligned} S\eta &= \eta^b - \eta^e = \frac{PRS^b}{TTP} - \frac{PRS^e}{TTP} && (3.16)\\ &= (1 - PER_L^b) - (1 - PER_L^e) && (3.17)\\ &= PER_L^e - PER_L^b. && (3.18) \end{aligned}$$

It is evident that all what we need to do now is to find Bob's average PER (PER_L^b) and Eve's one (PER_L^e) after L retransmission rounds, and then substitute them in (18) to find the net secure throughput. However, calculating PER of ARQ scheme analytically is not feasible as stated in the literature [57]. Although an approximate expression for the average PER of CC-HARQ after L^{th} round was recently given and discussed from the reliability and optimal power allocation perspectives in [58], but unfortunately it is not accurate at low SNR regimes. Moreover, from security point of view, Eve's performance comes into the picture, therefore, finding $S\eta$ requires not only finding exact Bob's PER, but also Eve's one. Motivated by all these factual challenges, we strive to find a simple closed-form expression for $S\eta$, which can practically reflect the achievable performance of the proposed security scheme.

By assuming that the effective SNR of the received combined signals at k^{th} round (i.e., accumulated SNR from all the retransmission rounds until the current k^{th} round) is defined by $\gamma_{b,\Sigma k} = \sum_{l=1}^{k}(\gamma_{b,l})$, whose joint probability density

function (PDF) is given by $g_{\gamma_b}(\gamma_{b,\Sigma k})$; and by defining error probability relating function as $f(\gamma_{b,\Sigma k})$, PER_L^b can be expressed as [58]

$$PER_L^b = \int_0^\infty ... \int_0^\infty f(\gamma_{b,\Sigma 1})...f(\gamma_{b,\Sigma L}) g_{\gamma_b}(\gamma_{b,1})...g_{\gamma_b}(\gamma_{b,L}) d\gamma_{b,1}...d\gamma_{b,L}. \tag{3.19}$$

According to [58], (19) can be simplified as follows:

$$PER_L^b = \int_0^\alpha g_{\gamma_b}(\gamma_{b,\Sigma L})\, d\gamma_b, \qquad \alpha = \int_0^\infty f(\gamma_b)\, d\gamma_b. \tag{3.20}$$

The difficulty of finding exact PER analytically is simplified when the effects of the retransmission parameters such as modulation, coding and combination are represented by a single transmission parameter. That is because α, which is called in the literature the waterfall threshold, can be taken from the simulation results of Bob's PER. Furthermore, α is related to a certain well-defined system model, which should be as close as possible to what happens in reality and the adopted parameters in the system design. Thus, α is a function of the transmission parameters, and is related to the instantaneous spectral efficiency (i.e. the accumulated information over a total number of transmitted information [λ]). Based on proposition (1) given in [58], PER_L^b can be written in terms of the cumulative distribution function (CDF) as

$$PER_L^b = F_{\gamma_b}^L(\alpha) = Pr\left(\sum_{k=1}^{L} \gamma_{b,k} < \alpha\right), \tag{3.21}$$

where $Pr()$ is the probability function, and $\sum_{k=1}^{L} \gamma_{b,k}$ is the sum of L statistically i.i.d. exponential random variables. More precisely, $\sum_{k=1}^{L} \gamma_{b,k}$ can be expanded as follows:

$$\sum_{k=1}^{L} \gamma_{b,k} = \gamma_{b,1} + \gamma_{b,2} + \cdots + \gamma_{b,L}\,, \tag{3.22}$$

$$= \bar{\gamma}_{b,1}|h_{b,1}|^2 + \bar{\gamma}_{b,2}|h_{b,2}|^2 + \cdots + \bar{\gamma}_{b,L}|h_{b,L}|^2\,, \tag{3.23}$$

where, $\bar{\gamma}_{b,1} = \bar{\gamma}_{b,2} = \cdots = \bar{\gamma}_{b,L}$, since equal modulation and power allocation during retransmission process are adopted. Also, the power of the channel gain ($|h_{b,k}|^2$) in Rayleigh fading environment at k^{th} round follows an exponential distribution with PDF $f(x) = \frac{1}{\bar{\gamma}} e^{-x/\bar{\gamma}}$.

Hence, the distribution of the sum given in (23) follows a Gamma distribution, $\Gamma(L,\gamma) \equiv \text{Gamma}(L,\gamma)$, and if k is a positive integer, which is always the case in our system, then the distribution turns out to be Erlang with CDF given as

$$F^{L}_{\bar{\gamma}_b}(\alpha) = 1 - \sum_{m=0}^{L-1} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_b}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}. \tag{3.24}$$

By substituting (24) into (21), we get the accurate generic PER^b_L formula as follows:

$$PER^b_L(\bar{\gamma}_b,\alpha) = 1 - \sum_{m=0}^{L-1} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_b}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}. \tag{3.25}$$

For the case of $L = 2$, Bob's PER becomes as below

$$PER^b_L(\bar{\gamma}_b,\alpha) = 1 - e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)} - \frac{\alpha}{\bar{\gamma}_b} e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}, \tag{3.26}$$

where α is derived numerically from the extensive simulation results, that we have performed at different modulation orders (M) and different L values [33]. Next, we carried out fitting methods on the obtained simulation results to get a simple formula for α, which can be represented as

$$\alpha = 2^{\lambda} - 1, \qquad \lambda = L \times \log_2(M) - 0.5, \qquad \lambda \geq 2.5. \tag{3.27}$$

The details of the simulation results used to perform curve fitting can be found in [33].

In the following, we present the analysis of Eve's PER denoted by PER^e_L first for the most two practical cases when $L = 2$ (related to voice service) and $L = 3$ (related to video service), and then in general for any L value. For voice service with $L = 2$, Eve's decoding error occurs when either 1) Eve's SNR in the first round is below the decoding threshold α, while Bob's one is above; or 2) when the accumulated SNR at Eve in the second round is still below the decoding threshold α, while Bob was below that threshold in the first round. Thus, Eve's PER can mathematically be written as

$$\begin{aligned} PER^e_L(\bar{\gamma}_e,\bar{\gamma}_b,\alpha) \;=\; & \underbrace{\left(F^1_{\bar{\gamma}_e}(\alpha)\right)}_{\text{Eve is in error at } k=1} \times \underbrace{\left(1 - F^1_{\bar{\gamma}_b}(\alpha)\right)}_{\text{Bob is in success at } k=1} \\ + \; & \underbrace{\left(F^2_{\bar{\gamma}_e}(\alpha)\right)}_{\text{Eve is still in error at } k=2} \times \underbrace{\left(F^1_{\bar{\gamma}_b}(\alpha)\right)}_{\text{Bob was in error at } k=1}, \; L = 2. \end{aligned} \tag{3.28}$$

It is obvious from (28) that Eve's PER not only depends on her channel condition, but also on Bob's channel and his success in decoding the packet before Eve is able to do so. After substituting the corresponding formulas of the CDFs into (28), Eve's PER becomes as

$$\begin{aligned} PER_L^e(\bar{\gamma}_e, \bar{\gamma}_b, \alpha) &= \left(1 - e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right) \times \left(e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right) \\ &+ \left(1 - \sum_{m=0}^{L-1} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_e}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right) \\ &\times \left(1 - e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right), L = 2. \end{aligned} \tag{3.29}$$

Finally, by substituting PER_L^e given in (29) and PER_L^b given in (25) into (18), we get the achievable secure throughput ($S\eta$) for the adaptive ARQ scheme without adding AN as follows:

$$\begin{aligned} S\eta &= \left(1 - e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right) \left(e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right) \\ &+ \left(1 - \sum_{m=0}^{L-1} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_e}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right) \left(1 - e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right) \\ &- 1 + \sum_{m=0}^{L-1} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_b}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}, L = 2. \end{aligned} \tag{3.30}$$

For the case of video service with $L = 3$, Eve's PER can mathematically be written as

$$\begin{aligned} PER_L^e(\bar{\gamma}_e, \bar{\gamma}_b, \alpha) &= \left(F_{\bar{\gamma}_e}^1(\alpha)\right) \times \left(1 - F_{\bar{\gamma}_b}^1(\alpha)\right) \\ &+ \left(F_{\bar{\gamma}_e}^2(\alpha)\right) \times \left(F_{\bar{\gamma}_b}^1(\alpha)\right) \times \left(1 - F_{\bar{\gamma}_b}^2(\alpha)\right) \\ &+ \left(F_{\bar{\gamma}_e}^3(\alpha)\right) \times \left(F_{\bar{\gamma}_b}^2(\alpha)\right), L = 3. \end{aligned} \tag{3.31}$$

After substituting the corresponding formulas of the CDFs into (31), Eve's PER becomes as

$$\begin{aligned} PER_L^e(\bar{\gamma}_e, \bar{\gamma}_b, \alpha) &= \left(1 - e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right) \times \left(e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right) \\ &+ \left(1 - \sum_{m=0}^{L-2} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_e}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right) \end{aligned}$$

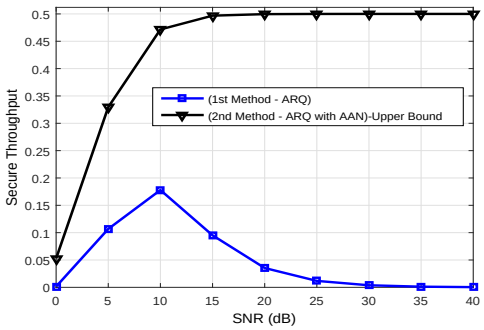


Figure 3.4: The achievable secure throughput using the derived analytical results for voice service for $\alpha = 4.66$, which corresponds to BPSK with $L = 2$ over a block Rayleigh fading channel. The curve colored with blue represents Eq. (30), while the one colored with black represents Eq. (33).

$$\times \left(1 - e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right) \times \left(\sum_{m=0}^{L-2} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_b}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right)$$
$$+ \left(1 - \sum_{m=0}^{L-1} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_e}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right)$$
$$\times \left(1 - \sum_{m=0}^{L-2} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_b}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right), L = 3. \quad (3.32)$$

Finally, by substituting PER_L^e given in (32) and PER_L^b given in (25) into (18), we can get the achievable secure throughput ($S\eta$) of the video service with $L = 3$.

For any service with any general L value, the generic formula of Eve's PER is also derived and given in the Appendix.

To get $S\eta$ under the adaptive AN-based method, we need to find the exact resulting distribution of γ_e, as well as to deliberately adjust the derived formula of α given in (27) by using fitting methods and according to the extra increase in the number of retransmissions caused due to the intentionally added AN. However, since finding the distribution of γ_e with AAN is extremely tedious and complex, we confine our analysis for the case of perfect secrecy, which holds when sufficient AN power is allocated so that Bob can decode the packet successfully only at the second retransmission round, i.e., $\eta_{new}^b = \frac{1}{2}\eta^b$, while Eve is kept unable to decode any information packets, i.e., $\eta^e = 0$. This can be achieved by assigning sufficient power to the added AN, as discussed in the previous section ($\varphi = SNR_{dB}$). The

upper bound of the achievable $S\eta$ for voice service ($L = 2$) can be given as

$$S\eta = \frac{1}{2}\eta^b = \frac{1}{2}\sum_{m=0}^{L-1}\frac{1}{m!}\left(\frac{\alpha}{\bar{\gamma}_b}\right)^m \left(e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right), L = 2. \tag{3.33}$$

It is of importance to notice here that the secure throughput is exactly equal to the legitimate user's throughput as perfect secrecy is achieved in this case, where Eve's throughput approaches zero while Bob can cancel the AN vectors and thus correctly decode the signal only in the second round. Fig. 3.4 shows the achievable secure throughput using the derived equations in (30) and (33). It is shown that ARQ with AAN method significantly outperforms that of ARQ alone due to the added AN.

3.5 ARQ with QoS-Based Adaptive Modulation

In addition to the usefulness and suitability of secure PER (i.e., the difference between Eve and Bob's PER performances) in cross-layers security design as it reflects the influence of upper layers' functions such as ARQ, it can also be linked with QoS requirements for various digital wireless applications such as voice, video, web browsing and so forth [1]. In particular, a previous knowledge of the type of running application at user side is a very advantageous feedback that should be taken into account during the phase of security design process to ensure conveying a certain service confidentially. This can be used as a solution for some cases, where securing a certain service is extremely needed at any distance from the base station (BS). More accurately, if Eve is closer to the BS than Bob (i.e., SNR value at Eve is higher than Bob, where Eve can receive the requested service with a quality better than Bob), then secure service is hard to be achieved. This situation is clearly visualized in Fig. 3.5 (a), where it is evident that secure voice communication for instance can not be achieved at (SNR$\geq$ 25) since Eve's PER is less than the minimum required QoS ($PER = 10^{-2}$) as indicated in [1]. This shows that the provided secrecy by the previous method (ARQ with MRC) is limited and might be insufficient in some cases where Eve may have better

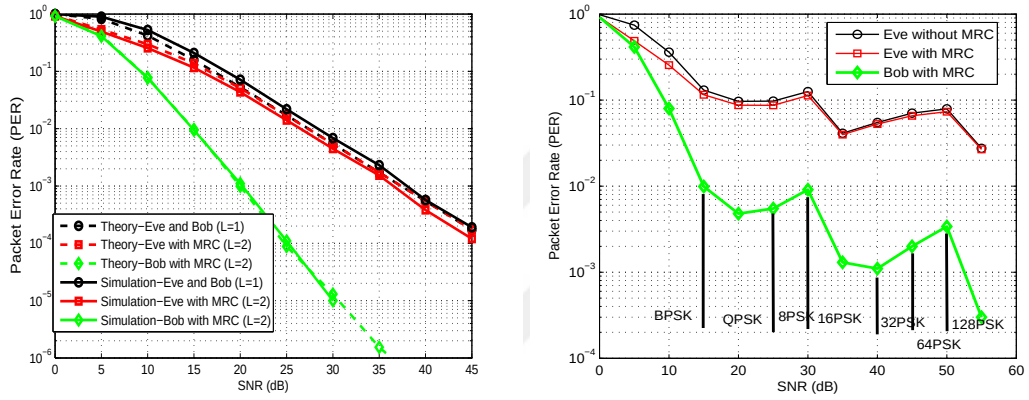
SNR Range	Modulation Type
SNR<20	BPSK
20<=SNR<25	QPSK
25<=SNR<30	8PSK
30<=SNR<36	16PSK
36<=SNR<42	32PSK
42<=SNR<47	64PSK
47<=SNR<58	128PSK

Table 3.2: Adaptive switching modulation table based on Bob's PER $\leq 10^{-2}$ (voice service).

SNR than Bob. To address this problem, we propose using adaptive modulation accompanied by ARQ to assure secure voice service against eavesdropping at any distance Eve may be located from the BS. Specifically, an accurate adaptive modulation switching table as shown in Table 3.2 is proposed to be used for providing guaranteed service-based security. More precisely, the modulation type is changed based on Bob's SNR in such a way that keeps Bob's PER less than a certain threshold related to the requested service, while Eve's PER is maintained to be greater than the that threshold. In this study, the proposed table is designed based on the QoS requirements associated with voice service as it will be shown in the next section. Keeping in mind that the same procedure can be used for securing other services such as video, which will have different adaptive tables. Although we have only targeted securing voice service in this paper, the same procedure followed in this context can be applied for securing other services such as video, messaging, web browsing and data streaming. However, these services will result in having different adaptive tables based on their QoS needs. Thus, further research has to be performed for finding security-based adaptive modulation tables for the rest of digital services that are defined in [1].

Fig. 3.5 (b) shows the exact obtained PER security performance using the proposed practical design (Bob's PER based-adaptive modulation table), where this method does not require any knowledge about Eve's channel. It is shown that Bob's PER is kept $< 10^{-2}$, while Eve's PER is kept $> 10^{-2}$, resulting in a secure voice service. It is also depicted that the Eve's PER behaviors with and

without MRC at high SNR regime are almost the same, since only a few packets are retransmitted based on Bob's channel, but not Eve. As a result, Bob's PER enhances, whereas Eve's PER has insignificant improvements.



(a) ARQ (b) ARQ with adaptive modulation

Figure 3.5: (a) Analytical and simulation results of ARQ (L=2) with BPSK. (b) Adaptive modulation process along with ARQ scheme (L=2).

3.6 Reducing PAPR and OOBE Besides Enhancing Secrecy in OFDM

The main objective of this section is to demonstrate how the new degree of freedom created by our proposed scheme in the power domain can intelligently be utilized to solve two major problems in the OFDM setup, while maintaining secrecy. As explained in Section III, to achieve secrecy, ARQ with MRC is exploited to add channel-based, QoS-guaranteeing, and null-space-independent AN that can inherently be canceled out at only the legitimate receiver by MRC. Besides secrecy, the added AN can be further exploited to attain other benefits. Specifically, the structure of the added AN can judiciously be redesigned to not only provide security, but also to reduce the PAPR and mitigate the OOBE in OFDM systems. Here, we reveal two new designs that can achieve the aforementioned goals. In the first design, the AN signal is optimized to reduce the PAPR

subject to a certain secrecy constrain defined by the power level of the added AN; while in the second design, the AN signal is redesigned to minimize the OOBE subject again to a certain power level that indirectly represents a well-defined secrecy constraint.

Also, it is worth mentioning that the deployment of the proposed security method in multi-carrier systems makes the method more resilient to eavesdropping as multi-path frequency selective channels in OFDM bring more randomness. Specifically, the randomness of the added channel-based AN in the OFDM case does not only come from the randomly generated samples at the transmitter, but also from the randomness of the multi-path frequency selective channel.

3.6.1 Joint PAPR Reduction and Physical Layer Security Design

In a basic OFDM, the transmitted time domain signal can be modeled as

$$\mathbf{d} = \mathbf{G}\mathbf{F}^H\mathbf{s} \in \mathbb{C}^{[(N+T-1)\times 1]}, \tag{3.34}$$

where $\mathbf{s} \in \mathbb{C}^{[N\times 1]}$ is a set of QAM symbols in frequency domain, $\mathbf{F}^H$ is the N-point inverse discrete Fourier transformation (DFT) matrix, and $\mathbf{G} \in \mathbb{C}^{[(N+T-1)\times N]}$ is the CP addition matrix, where T is the number of channel taps. Unlike [50], [65], which adds the AN in the time domain of the signal by exploiting the channel's null-space, in the proposed design, the newly designed AN signal $\mathbf{z} \in \mathbb{C}^{[N\times 1]}$ is added on top of the data symbols in the **frequency** domain by exploiting ARQ with MRC process, which is performed in the **frequency** domain too. Thus, the newly proposed transmitted signal can be written as

$$\mathbf{d} = \mathbf{G}\mathbf{F}^H(\mathbf{s} + (\mathbf{H}_f\mathbf{H}_f^H)^{-1}\mathbf{z}) \in \mathbb{C}^{[(N+T-1)\times 1]}, \tag{3.35}$$

where $\mathbf{H}_f \in \mathbb{C}^{[N\times N]}$ is the diagonal matrix of the channel frequency response with diagonal entries $\{H_1, H_2, \cdots, H_N\} \in \mathbb{C}^{[1\times N]}$. The baseband PAPR of the above-transmitted signal is the ratio between the maximum transmitted power

and the average power, which can be given as

$$PAPR = \frac{\|\mathbf{G}\mathbf{F}^H(\mathbf{s} + (\mathbf{H}_f\mathbf{H}_f^H)^{-1}\mathbf{z})\|_\infty^2}{\frac{1}{N+T-1}\|\mathbf{G}\mathbf{F}^H(\mathbf{s} + (\mathbf{H}_f\mathbf{H}_f^H)^{-1}\mathbf{z})\|_2^2}. \tag{3.36}$$

The problem here reduces to finding the optimal AN vector $\mathbf{z}$ that can reduce the PAPR. Thus, the optimization problem to be solved can be formulated as follows:

$$\begin{aligned} \mathbf{z} = \arg\ \min_{\mathbf{z}} & \|\mathbf{G}\mathbf{F}^H(\mathbf{s} + (\mathbf{H}_f\mathbf{H}_f^H)^{-1}\mathbf{z})\|_\infty^2 \\ & subject\ to \rightarrow \|\mathbf{z}\|_2^2 \leq \frac{\lambda \times \|\mathbf{s}\|_2^2}{\|(\mathbf{H}_f\mathbf{H}_f^H)^{-1}\|_2}, \end{aligned} \tag{3.37}$$

where the percentage of the power used by the AN signal is controlled by $\lambda \in [0, 1]$ to achieve a certain pre-defined secrecy level, while making the PAPR as minimal as possible[4] The objective function shows that we have a convex optimization problem that can numerically be solved by one of the advanced and powerful optimization solvers such as MOSEK. In this case, to obtain a precise numerical solution to (37), we adopt using YALMIP, a handy optimization package that can smoothly be integrated with MOSEK and MATLAB to solve complex optimization problems. The PAPR performance results of this design will be shown in Section VI.

3.6.2 Joint OOBE Reduction and Physical Layer Security Design

Now, we turn our attention to reduce the OOB power leakage by redesigning and optimizing the AN structure subject to a secrecy constraint defined by the power level of the added AN. Before we start with the design, we need first to determine

[4]It should be emphasized that the optimization problem can be reformulated in another way, i.e., to design the AN that maximizes the secrecy performance subject to a certain PAPR constraint. However, since the resulting problem formulation in this case would be non-convex (has no solution) and also may seem impractical as it requires Eve's channel, we instead formulate the problem of minimizing the PAPR (which is a hardware limiting factor, where it may impede the implementation of the security technique if it does not comply with it) subject to a certain power constraint on the added AN, which indirectly resembles the targeted secrecy performance.

the main signal spectrum and the interfering part of the signal. The spectrum of the transmitted OFDM signal can be given as

$$\mathbf{S}_{\zeta N} = \|\mathbf{F}_{\zeta N}\left(\mathbf{G}\mathbf{F}^{H}\mathbf{M}(\mathbf{s} + (\mathbf{H}_f\mathbf{H}_f^{H})^{-1}\mathbf{z})\right)\|_2^2, \tag{3.38}$$

where, $\mathbf{M} \in \mathbb{C}^{N\times N_s}$ is a sub-carrier mapping matrix containing the N_s columns of $\mathbf{I}_N$ corresponding to the active data sub-carriers. Also, $\mathbf{F}_{\zeta N}$ is an $\zeta N \times (N+T-1)$ DFT matrix, in which ζ is the oversampling factor used optionally to increase the resolution of the measured spectrum. Now, if we consider that there are ν sub-carriers, which are deactivated from the edge band of the OFDM signal spectrum, then the interference in the edge band can be given as

$$\mathbf{I}_{\nu} = \|\mathbf{F}_{\nu}\left(\mathbf{G}\mathbf{F}^{H}\mathbf{M}(\mathbf{s} + (\mathbf{H}_f\mathbf{H}_f^{H})^{-1}\mathbf{z})\right)\|_2^2, \tag{3.39}$$

where $\mathbf{F}_{\nu}$ is a sub-matrix of $\mathbf{F}_{\zeta N}$, and comprised of only the rows that are related to the sub-carriers set as a guard band, or occupied by an edge user. To minimize the interference leakage in the edge band, we formulate the following optimization problem that has to be solved for $\mathbf{z}$

$$\begin{aligned}\mathbf{z} = \arg\min_{\mathbf{z}} \|\mathbf{F}_{\nu}\left(\mathbf{G}\mathbf{F}^{H}\mathbf{M}(\mathbf{s} + (\mathbf{H}_f\mathbf{H}_f^{H})^{-1}\mathbf{z})\right)\|_2^2 \\ subject\ to \rightarrow \|\mathbf{z}\|_2^2 \leq \frac{\lambda \times \|\mathbf{s}\|_2^2}{\|(\mathbf{H}_f\mathbf{H}_f^{H})^{-1}\|_2}.\end{aligned} \tag{3.40}$$

The solution to this problem can numerically be obtained using efficient optimization solvers. Here, we again select MOSEK as our solver due to its efficiency and accuracy.

The effectiveness of the proposed optimization problems in reducing PAPR and OOBE of OFDM will be exhibited in the next section by using computer simulations. Future work regarding this section can include conducting thorough investigation and analysis alongside finding analytical closed-form solutions for the above formulated problems.

3.7 Simulation Scenario and Results

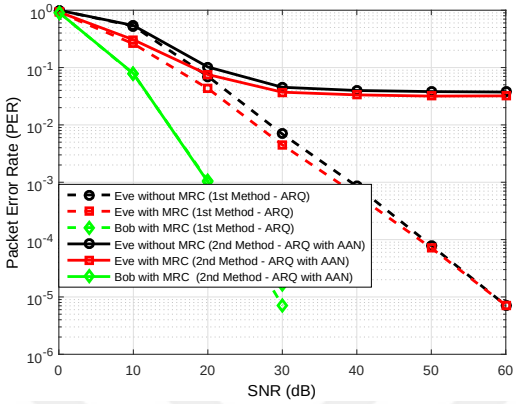
The simulation results are divided into three phases: the first is related to ARQ with MRC; the second is associated to ARQ with MRC and AN; whereas the third is concerned to PAPR and OOBE in OFDM system using the aforementioned formulated optimization problems that are based on the proposed ARQ with AN design. The adopted system specifications for the first two phases are listed in Table 3.3. To investigate the obtained performance; average PER as

Table 3.3: System specifications

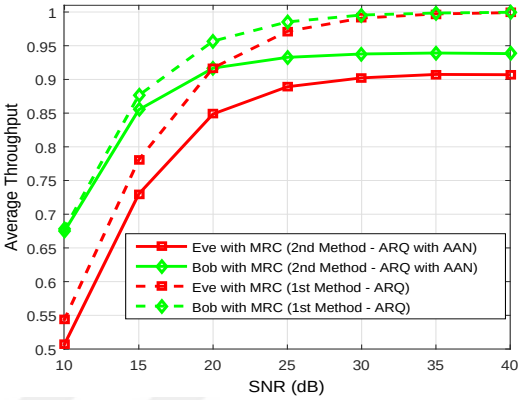
Parameter	**Setting Value**
Maximum number of retransmission (L)	2 (for voice), 3 (for video)
Packet size	432 symbols
CRC Size	32 bits
Modulation	BPSK
Receiver structure	MRC on a symbol level basis
Channel type	Block Rayleigh fading, where retransmitted packets experience independent channel gains [42]

well as average throughput of both Bob and Eve, secure throughput, and the delay caused by the adopted ARQ scheme; are all evaluated and characterized. Thus, a comprehensive picture of the whole system performance is drawn, which eventually helps not only in quantifying the achievable performance, but also in understanding the trade-off among the different service requirements in terms of secrecy, reliability, throughput, and delay.

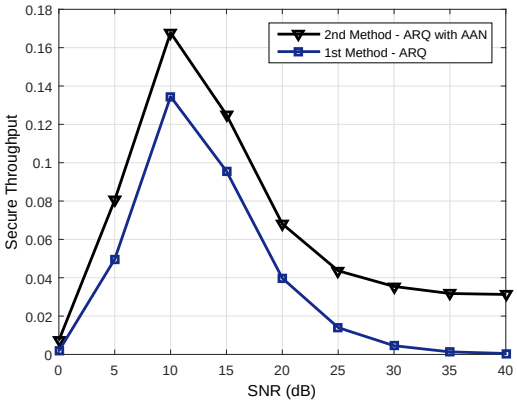
In Fig. 3.6 (a), voice service with L=2 is targeted to be secured. It is evident that there is a PER secrecy gap between Bob and Eve at comparable SNRs due to the implicit adaptivity resulting from ARQ along with MRC, which is basically in favor of Bob but not Eve as explained earlier. This happens because Bob can ask for retransmission according to his channel conditions, while Eve cannot. Although ARQ with MRC can provide a noticeable PER secrecy gap, it is insufficient for providing a secure voice service at high SNRs because Eve's PER becomes less than a certain threshold needed for using the voice service



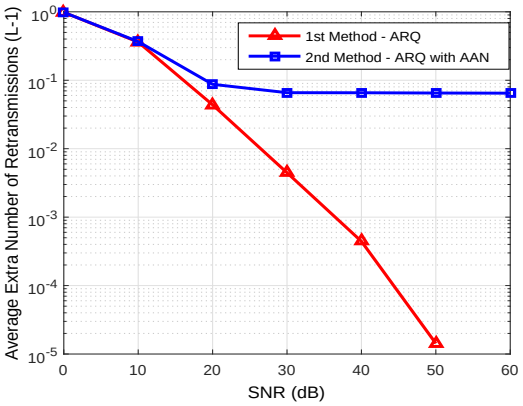
(a) Packet Error Rate (PER) vs SNR



(b) Average Throughput vs SNR



(c) Secure Throughput vs SNR



(d) Delay (L-1): Average retransmission percentage vs SNR

Figure 3.6: Reliability, security and throughput performance comparison between ARQ without and with AAN with $\varphi = 0.01$ for providing a secure voice service (L=2).

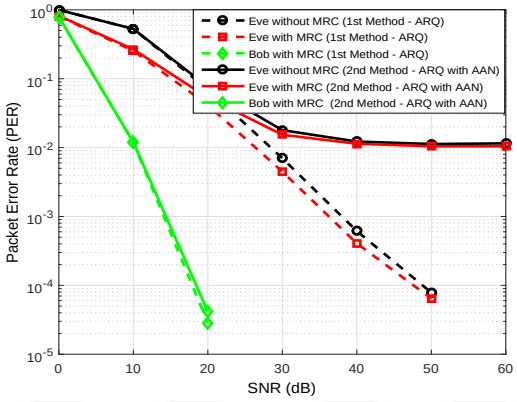
reliably. More specifically, at SNR values above 30 dB, Eve's PER becomes less than 10^{-2}, therefore voice service becomes insecure as Eve can reliably decode the service. To combat this problem, the proposed method, ARQ with AAN, is used, where we add to the data packet an AAN that is designed based on the QoS and the channel between the legitimate parties. Thus, in the second part of our simulations, the AAN block shown in Fig. 3.2 is switched on. Now, AAN is added according to the QoS requirements of the voice service, which is determined (as reported in LTE standard) in terms of PER being $\leq 10^{-2}$ and L being ≤ 2 as presented in Table 3.1, where packet delay budget is determined

to be less than 100 ms [1]. Fig. 3.6 (a) shows the PER performance of the new proposed method. It is clear that the gap between Bob and Eve is significantly increased. Consequently, voice service is now secured at any SNR Eve may have (i.e., at any distance Eve may be located from the base station). However, Fig. 3.6 (b) shows that the proposed AAN-based method is accompanied by a slight throughput degradation due to the tiny increase in the average extra number of retransmissions ($L-1$). This can be explained by the fact that adding AN will mostly cause receiving the first transmission round of each packet in error, which will force Bob to ask for retransmission to cancel the added AN. Fig. 3.6 (c) depicts that ARQ with AAN method not only increases secrecy, but also ensures it at high SNR values unlike ARQ alone. Fig. 3.6 (d) presents the exact effect of the proposed method on increasing the average extra number of retransmissions, where it is exhibited that the resulting gain in the secure throughput comes at the expense of a tiny increase in the percentage of the retransmitted packets, which anyway lies within the QoS requirements of the voice service.

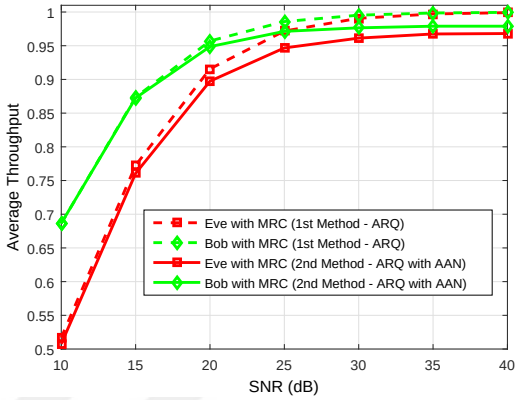
Fig. 3.7 is devoted to illustrate the exact obtained performance using the proposed design for conversational (live streaming) video service (L=3) [1]. Here, we add AN only to the first and second rounds, while the third round is left free of noise. It is made like this to balance the added AN so that it gets canceled after MRC process. In Fig. 3.7 (a), it is exhibited that Bob's PER is kept $< 10^{-3}$ with respect to the QoS requirement of the video service as presented in Table 3.1, while Eve's PER is kept $> 10^{-3}$, resulting in a secure video service at any SNR. Fig. 3.7 (b) shows that the throughput degradation in case of video service is less than that of voice since lower AN power is added ($\varphi = 0.001$). Fig. 3.7 (c) confirms that secrecy has been maintained even at high SNR. Fig. 3.7 (d) shows the extra small delay caused in case of using the second method. It is depicted that at SNR ≥ 30 dB, the receiver asks the retransmission of only one packet out of each 100 packets[5] to cancel the effect of the added AN so that secure video service can be achieved. Thus, security is achieved without exceeding the QoS requirements of the targeted service.

Fig. 3.8 and Fig. 3.9 present the comprehensive performance of the proposed

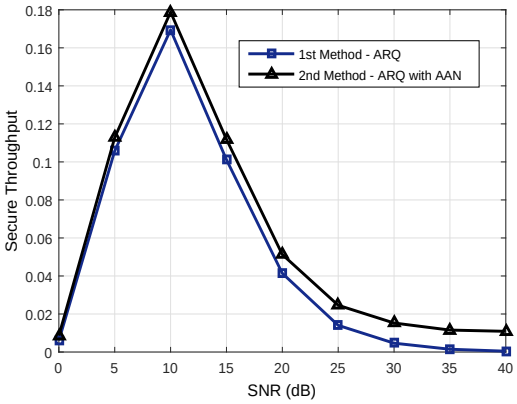
[5]This is because the power of the added AN is so small ($\varphi = 0.001$ from Table 3.1) that it does not even harm Bob's reception in most of the cases, while it is significantly impacting Eve's performance.



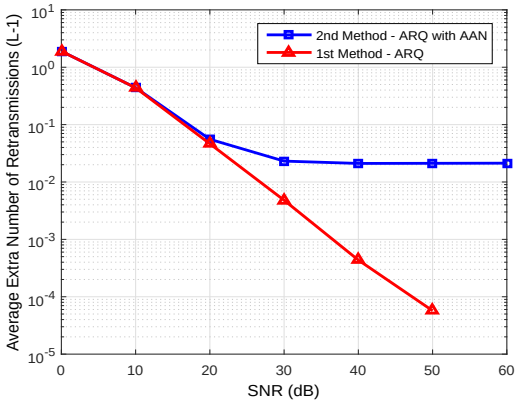
(a) Packet Error Rate (PER) vs SNR



(b) Average Throughput vs SNR



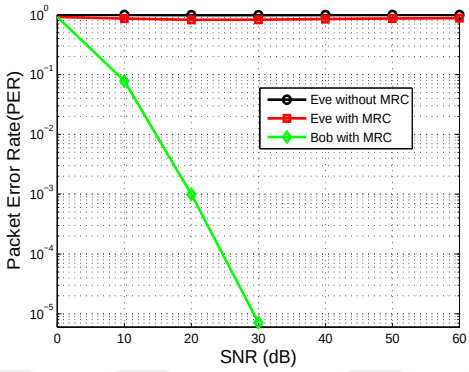
(c) Secure Throughput vs SNR



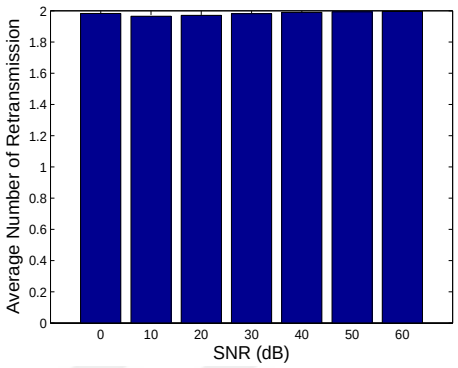
(d) Delay (L-1): Average retransmission percentage vs SNR

Figure 3.7: Reliability, security and throughput performance comparison between ARQ without and with AAN with $\varphi = 0.001$ for providing secure video service (L=3).

method in case of TCP-based services such as web browsing, E-mail, chatting, messaging, FTP, P2P file sharing, etc. Since the content of all these services is basically text, it is highly desirable from a practical point of view to perfectly secure it. This is because of the fact that any information leakage will explicitly cause disclosing some text content to the eavesdropper, who is capable of doing complex processing to guess what was the content. To achieve this, Eve's PER should be as close as possible to unity (worst performance), which results in zero throughput to Eve, i.e., perfect secrecy. Such a target is shown to be achievable by our proposed method through allocating sufficient noise power ($\varphi = SNR_{dB}$)



(a) Packet Error Rate (PER) vs SNR

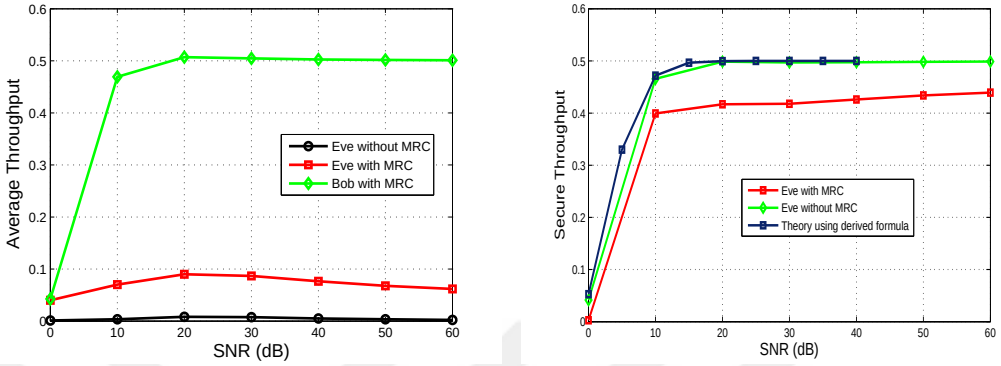


(b) Average number of retransmissions (L)

Figure 3.8: Reliability performance comparison between Bob and Eve when sufficient AN power is added to provide close to perfect secrecy at (L=2).

to the two rounds (L=2). Specifically, Fig. 3.8 (a) shows the PER performance comparison between Bob and Eve. It is clear that Eve's PER is exactly one without MRC, and around 0.9 (very close to one) with MRC. In Fig. 3.7 (b), it is pictured that the average number of retransmissions (L) for all SNR values is almost 2 as expected due to the added high AN power. On the other hand, throughput and secrecy performance comparison between Bob and Eve is drawn in Fig. 3.9, where it is evident that the secure throughput performance shown in Fig. 3.9 (b) is almost the same as Bob's average throughput shown in Fig. 3.9 (a). From these comparisons, it is obvious that the degradation in the legitimate receiver's throughput turns out to be a secure throughput in the case of perfect secrecy, which is needed for messaging and web services. Moreover, Fig. 3.9 (b) exhibits that the analytically derived equation of the upper bound secure throughput given in (33) matches the obtained simulation results. Thus, without exceeding L set by the protocol nor degrading PER performance of the legitimate user, a practically perfect secure service transmission is achieved.

Finally, to show the effectiveness of the proposed method in mitigating PAPR and OOBE besides security in multi-carrier systems, the method is used and simulated in a standard OFDM system. In this system, the number of sub-carriers is set to 64 and the CP length is set to be equal to the channel spread length. Fig. 3.10 shows the PAPR performance of the OFDM system that uses the proposed



(a) Average Throughput vs SNR (b) Secure Throughput vs SNR

Figure 3.9: Throughput and security performance comparison between Bob and Eve using sufficient AN power to provide perfect secrecy at (L=2).

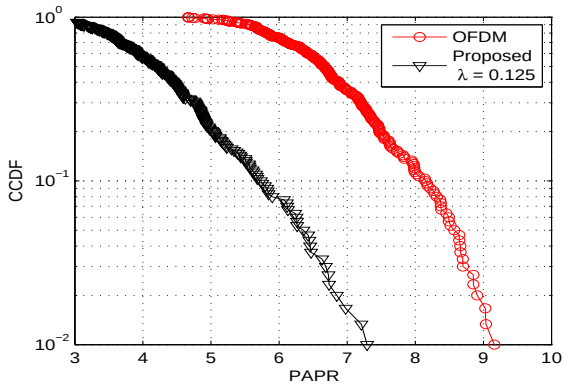


Figure 3.10: CCDF of baseband PAPR, where the proposed security design is exploited for reducing PAPR.

joint MAC/PHY design of ARQ with AN compared with a conventional OFDM that does not use the proposed AN design. Note that the AN vector in this case is obtained from the solution of the optimization problem formulated in (37). It is clear that there is a remarkable PAPR reduction due to the adoption of our proposed method.

In order to evaluate the capability of the proposed method in reducing OOBE, we assume that there is an adjacent user transmitting its OFDM signal over 16 subcarriers located at the edge of the OFDM transmission band. Fig. 3.11 shows the OOBE performance of an OFDM scheme that uses the proposed ARQ with AN design, compared with the conventional OFDM. Note that the AN vector in

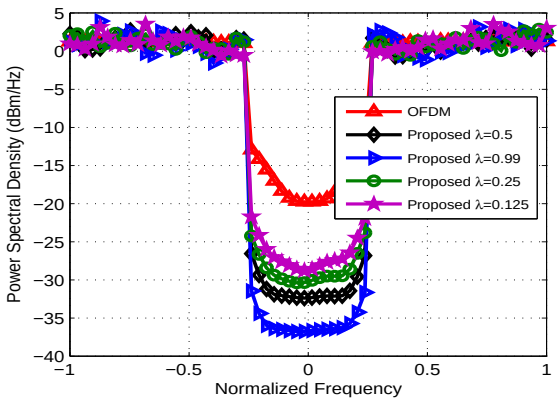


Figure 3.11: Out-off-band emission (OOBE) reduction performance at different λ values, where the proposed security design is utilized to reduce OOBE. The number of deactivated sub-carriers (ν) is one forth of the total number of sub-carriers (N).

this case is obtained from the solution of the optimization problem formulated in (40). It is clear that there is a significant reduction in OOBE due to the adoption of our proposed method. It is also shown that as we increase λ (the power of the added AN signal with respect to the power of the transmitted OFDM signal), the OOB interference reduces more.

3.8 Conclusion

A practical, effective, and cross PHY-MAC layer security method is proposed for securing any service requested by legitimate users. Particularly, ARQ along with MRC and AN have jointly been exploited to develop an eavesdropping-resilient system. This has been achieved by intentionally adding a properly well-designed channel amplitude-dependent, null-space-independent, PAPR-aware, and QoS-based (adaptive) AN on top (superimposed in the power domain) of the transmitted data packets in such a way that the added AN vectors cancel each other at only the legitimate receiver, while severely deteriorating Eve's performance. It has been shown that without exceeding the QoS requirements set by the current LTE standard, and without degrading PER performance of the legitimate user,

perfect secure service transmission can be achieved. For some services such as voice and video, it is observed that secure transmission can be attained by just forcing Eve to operate below the defined QoS requirements (unsatisfied QoS for Eve). Thus, security is guaranteed without sharing a secret key, nor imposing any changes in the receiver structure, making it a very suitable candidate technique for future 5G and beyond wireless networks as well as for low complexity Internet of Thing (IoT) devices. Besides, the proposed scheme is shown to help reduce the PAPR and OOBE of OFDM-based waveforms.

Future work may include the following research items for future studies: 1) Extension of the proposed concept to other domains and scenarios, where diversity exists and combination can be used to restore the data. These scenarios include MIMO with spatial multiplexing MIMO with space time block coding (STBC), MIMO with spatial modulation, coordinated multi-point (CoMP), distributed antenna systems (DAS), cooperative relays, etc. 2) Detailed performance investigation and quantifications of the proposed method under the effect of different fading channel models and with various coding schemes such as polar code.

Chapter 4

OFDM with Subcarrier Index Selection and Adaptive Interleaving for Improving Security and Reliability of 5G URLLC Services

4.1 Introduction

The broadcast nature of communication systems makes wireless transmission susceptible to passive eavesdropping, endangering the secrecy of data-carrying signals. Traditionally, data confidentiality has been tackled using encryption and cryptography-based approaches. However, due to the huge advancement in future 5G and beyond wireless networks, featured by the ability to serve massive amount of devices with diverse requirements and applications, cryptography-based approaches may no longer remain an adequate way to provide security [2]. This is due to the fact that encryption entails key generation, distribution, and management processes, which are extremely challenging tasks especially in dynamic,

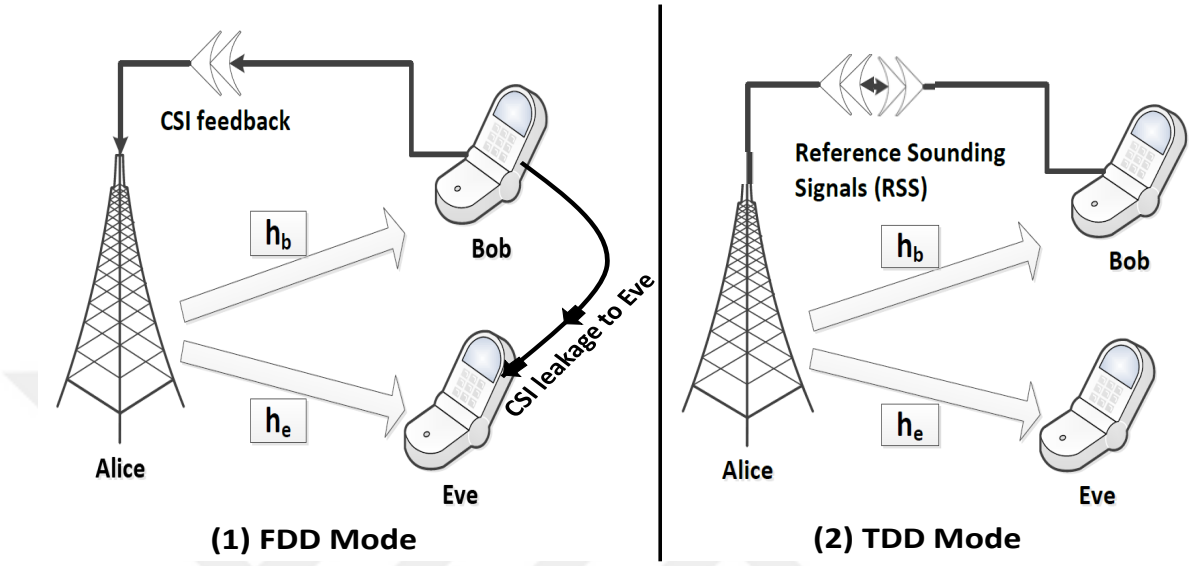


Figure 4.1: A simplified generic system model for the considered two physical layer security scenarios: 1) FDD mode, where the CSI of Bob is sent publicly to Alice, enabling Eve to access it. 2) TDD mode, where the CSI of Bob is estimated by using channel sounding, preventing Eve from accessing it.

multi-heterogeneous networks with massive device connections.

To cope with this, key-less physical layer security (PLS) has emerged as a new concept and powerful alternative that can complement and may even replace encryption-based approaches [6], [38]. The basic idea is to exploit channel characteristics alongside well-designed transmission schemes in order to ensure the ability of the intended user to perform successful data decoding, while preventing eavesdroppers from doing so [6], [56]. In the literature, practical signal processing-based security techniques are shown to be among the effective ways in providing secrecy. This can be performed, for-instance, by utilizing the degree of freedom that exists in the space domain like MIMO, coordinated multi-point (CoMP), relay, etc. However, when there is no spatial degree of freedom, exploiting the time and frequency degrees of freedom of the transmit waveforms becomes of significant importance to safeguard wireless transmission against eavesdropping. Moreover, since OFDM is the most commonly used waveform in currently existing systems and is expected to keep its dominance with various numerologies in future 5G systems [66], securing OFDM waveform has drawn the attention of many researchers in recent times. It is worth mentioning that besides developing

techniques tailored to common transmit waveforms like OFDM, there have recently been some efforts to design new inherently secure waveforms as in [67], [52].

In the literature, several OFDM-based security techniques have been proposed. These techniques can be categorized from a high-level viewpoint into four main enabling schemes. First, secret key-based schemes, in which secret random sequences are generated from the channel and then used to encrypt the transmitted data on either the application layer [68] or the physical layer such as dynamic coordinate interleaving and constellation rotation schemes [69]. Second, adaptive transmission-based schemes, in which the transmission parameters are adjusted to just meet the quality-of-service (QoS) requirements of only the legitimate receiver. Among these techniques are optimal power allocation [70], adaptive modulation with hybrid-automatic-repeat-request (HARQ) [33], adaptive precoding and interleaving [53], fading-based subcarrier deactivation schemes [49], channel shortening [71], etc. Third, artificial noise (AN)-based schemes [50], in which AN is designed based on the legitimate receiver's channel so that it only harms the eavesdropper's reception, while maintaining an interference-free reception at the legitimate user. Fourth, schemes that can exploit OFDM transceiver impairments [72] or conceal some key features in the OFDM signal to provide secrecy [51].

As inferred, most of the aforementioned OFDM-tailored PLS designs were introduced without having the special requirements of 5G services in mind. Particularly, ultra-reliable and low-latency communication (URLLC) [73], which is expected to be a critical service in 5G networks, imposes new requirements when the PLS design is considered. For URLLC services, physical layer secrecy is desirable to be achieved, while providing better reliability and power efficiency with minimal complexity and low latency. Besides, the security technique has to work in practical scenarios where a reliable channel state information (CSI) feedback may be required to be publicly sent to the transmitter, allowing the eavesdropper to access it and thus causing CSI leakage [74, 75], which is the case in frequency division duplexing (FDD) systems. These new requirements make many of the OFDM-based security techniques unsuitable for 5G URLLC scenario; mainly because of the needed complexity and significant changes in the transceiver design

without providing any extra benefits in terms of: 1) reliability, 2) power efficiency, 3) certain robustness to the legitimate CSI leakage, and/or 4) eliminating the need for the knowledge of the eavesdropper's channel at the transmitter.

To address the above challenges, in this chapter, inspired by OFDM with index modulation (OFDM-IM) [76–78], where the whole OFDM block is divided into sub-blocks and only a subset of the available subcarriers is used for transmission in each block, we first propose an effective physical layer security scheme called OFDM with subcarrier index selection (OFDM-SIS) by exploiting the principle of subcarrier selection in a different manner to enhance the confidentiality performance and guarantee a good level of secrecy gap even in the FDD mode. In the proposed scheme, the frequency response of correlated subchannels is first converted into a completely uncorrelated effective response by means of adaptive channel-based interleaving. Then, only the subcarriers corresponding to high sub-channel gains in each sub-block are used for data transmission in order to maximize the signal-to-noise ratio (SNR) at only the legitimate receiver, while the rest are nulled and not used for data transmission. Interestingly, the presented design is found out to not only provide secrecy in the worst security scenario, but also to enhance the bit error rate (BER) performance of the legitimate receiver, where a significant gain is obtained while saving the transmit power.

Next, we investigate the enhancement in the secrecy performance that can be achieved by the proposed scheme when time division duplexing (TDD) mode is considered. This is achieved by introducing two levels of security, which are obtained by the joint and hybrid design of subcarrier index selection alongside adaptive interleaving based on the channel of the legitimate user. This scheme is named as OFDM-SIS with adaptive interleaving (OFMD-SIS-AI). Next, we propose a method for avoiding channel reciprocity mismatch that may result from having non-reciprocal hardware components in the transceiver chain or experiencing different levels of interference in the uplink and downlink.

Moreover, to facilitate the BER and outage secrecy performance analysis of the proposed OFDM-SIS scheme, the probability distribution functions (PDFs) of the effective instantaneous power and amplitude of the faded subchannels are numerically calculated using fitting methods. Based on these, new mathematical expressions for the BER of both the legitimate receiver and the eavesdropper as

well as the secrecy outage probability are derived. The provided results prove the effectiveness of the proposed design in achieving practical secrecy alongside remarkable enhancement in the BER performance of the legitimate receiver with respect to the conventional and index modulation-based OFDM designs.

The rest of the paper is organized as follows. The system model and its

Table 4.1: The two operational modes considered in the system model.

	(1) **FDD mode**	(2) **TDD mode**
Scenario description	The CSI of Bob is sent publicly to Alice, enabling Eve to access it (CSI leakage to Eve).	The CSI of Bob is estimated by using channel sounding reference signals, preventing Eve from accessing it (no CSI leakage).
Enabling security technique	Optimal subcarrier index selection in each sub-block to maximize the SNR at Bob only. The technique is named as OFDM-SIS.	Joint optimal subcarrier index selection and adaptive interleaving based on the channel of Bob, resulting in two levels of security. The technique is renamed as OFDM-SIS-AI.
Evesdropper status	Since Eve knows the channel of the legitimate user from the explicit feedback, she is assumed to know the selected subcarriers as well as the used interleaver.	Since Eve does not have the knowledge of the legitimate user's channel as there is no explicit feedback (i.e., channel sounding is used to estimate the channel by exploiting channel reciprocity), she has no knowledge of the used interleaver.

preliminaries are described in Section 4.2. The details of the developed secure OFDM-SIS scheme are revealed in Section 4.3. The explanation and illustration of the proposed method used for avoiding channel reciprocity mismatch is given in Section 4.4. The analytical analysis is presented in Section 4.5. Computer simulation results are exhibited and discussed in Section 4.6. Finally, the paper is concluded in Section 4.7.[1]

4.2 System Model and Preliminaries

A single-input single-output (SISO) OFDM system is considered. Specifically, the system is composed of a transmitter (Tx), called Alice, aims at communicating confidentially with a legitimate receiver (Rx), called Bob, whereas an eavesdropper, called Eve, is trying to intercept the data communication link between the two legitimate parties (Alice and Bob) as shown in Fig. 4.1, where two operational modes (FDD and TDD) are considered for the proposed scheme. The channels experienced by both Bob $\mathbf{h_b} \in \mathbb{C}^{[1\times L]}$ and Eve $\mathbf{h_e} \in \mathbb{C}^{[1\times L]}$ are assumed to be multi-path slowly varying channels with L exponentially decaying

[1] *Notations*: Vectors are denoted by bold-small letters, matrices are denoted by bold-capital letters, and $\mathbf{I}$ is the identity matrix. The transpose, Hermitian, and inverse are symbolized by $(\cdot)^{\mathrm{T}}$, $(\cdot)^{\mathrm{H}}$ and $(\cdot)^{-1}$, respectively.

taps with Rayleigh fading distribution. Moreover, since Eve is a passive node, the realistic assumption, where Alice has no knowledge of Eve's channel, is adopted. Moreover, both Bob and Eve are assumed to experience independent channels as the wireless channel changes according to the locations of Tx and Rx as well as the environment [52]. In addition, we assume two operational division duplexing modes, whose scenario descriptions, proposed enabling security techniques, and Eve's status for each mode are summarized in Table 4.1.

At Tx, the number of frequency-domain complex data symbols to be transmitted is N, which also represents the total number of utilized subcarriers. Thus, we represent the frequency-domain OFDM symbol as $\mathbf{s} = \begin{bmatrix} s_0 & s_1 & ... & s_{N-1} \end{bmatrix}^{\mathrm{T}} \in \mathbb{C}^{[N \times 1]}$. The OFDM symbol is then interleaved in order to eliminate the correlation between the subchannels and make them look completely random and independent as shown in Fig. 4.2. This is performed so that we can ensure distributing the deep-faded subchannels uniformly over the whole OFDM symbol, and thus guarantee to experience a few deep-faded subchannels in each subblock. In this work, we consider using an adaptive CSI-dependent interleaver, denoted by a unitary matrix $\mathbf{R}$ of size $N \times N$, where the entries of each column are all zeros except a single entry of value equals to one at the position of the subcarrier to be permutated [53]. We select CSI-based interleaving for two reasons: 1) it is proven to be the best in terms of eliminating burst errors (or consecutive deep-faded subchannels) and make them uniformly distributed over the whole OFDM block when the CSI is available at Tx [79]; 2) it can be utilized to provide a second level of security in TDD mode beside the level obtained by the optimal subcarrier index selection process [53]. It is worth mentioning that the interleaver design that we have recently devised in [53] was perceived as a kind of precoder due to the fact that $\mathbf{R}$ was extracted by applying singular value decomposition on the diagonal matrix of the channel amplitude frequency response, and then taking the right unitary matrix, resulting from the decomposition, as the interleaving matrix. For more details on the design of this type of interleavers and how it can be made robust to channel reciprocity mismatch, we refer the readers to [53] and [79]. Another important detail to mention here is the fact that Eve is assumed to perfectly know $\mathbf{R}$ in FDD mode as the CSI is publicly sent from Bob to Alice, and thus, Eve can use this CSI to derive the used interleaver $\mathbf{R}$. Similar to

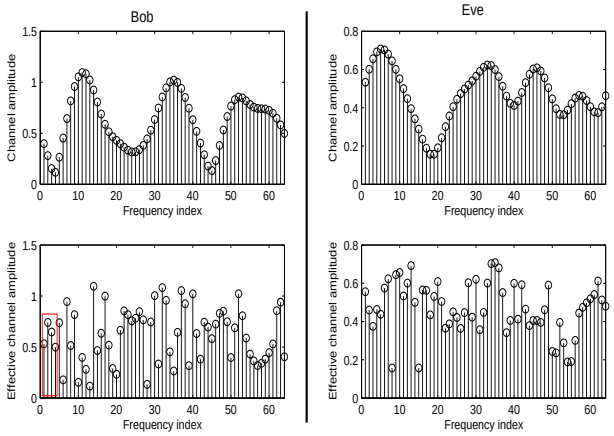


Figure 4.2: Bob's and Eve's channel frequency responses alongside their effective interleaved channels i.e., $\mathbf{H_b^f R}$ and $\mathbf{H_e^f R}$ (shown in lower part of the figure).

OFDM-IM [76], where the whole OFDM block is divided into sub-blocks and only a subset of the available sub-carriers in each sub-block is used for data transmission, here we follow a similar procedure; however, in our technique, the subcarrier indices are not used to convey information, but rather selected adaptively based on the channel of the legitimate receiver to provide secrecy and enhance reliability. This is different from OFDM-IM, where the sub-carriers are selected based on the incoming data to convey information by the sub-carrier indices so that better reliability can be achieved at the expense of a minor spectral efficiency loss. The details of the proposed OFDM-SIS security technique along with its physical structure will be explained in the next section. The resulting interleaved block ($\mathbf{g} = \mathbf{Rs}$) is then passed through an IFFT process $\mathbf{F}^{\mathrm{H}} \in \mathbb{C}^{[N\times N]}$, which basically maps the data points to orthogonal sub-carriers, where $\mathbf{F}$ is the discrete Fourier transform matrix. To avert the inter-symbol-interference, a cyclic prefix (CP) of length L is inserted by using the CP appending matrix $\mathbf{C} \in \mathbb{R}^{[(N+L)\times N]}$. Thus, the transmitted baseband signal by Alice can be represented as

$$\mathbf{x} = \mathbf{CF}^{\mathrm{H}}\mathbf{Rs} = \mathbf{CF}^{\mathrm{H}}\mathbf{g} \in \mathbb{C}^{[(N+L)\times 1]}. \tag{4.1}$$

After the signal $\mathbf{x}$ passes through the channel and reaches both Bob and Eve, each one of them will first discard the CP part of the signal using the matrix of $\mathbf{D} \in \mathbb{R}^{[N\times(N+L)]}$ and then perform an FFT process using the matrix of $\mathbf{F} \in \mathbb{C}^{[N\times N]}$ to transform the signal into the frequency domain. Thus, the net received

signal vector with dimensions $N \times 1$ at Bob after performing the aforementioned operations can be given in a linear matrix representation form as follows

$$\begin{aligned} \mathbf{y_b} &= \mathbf{FD}\left(\mathbf{H_b C F^H R s} + \mathbf{z_b}\right) && (4.2) \\ &= \mathbf{H_b^f R s} + \hat{\mathbf{z}}_\mathbf{b}. && (4.3) \end{aligned}$$

On the other hand, at Eve, the captured signal after the FFT process can be formulated as

$$\begin{aligned} \mathbf{y_e} &= \mathbf{FD}\left(\mathbf{H_e C F^H R s} + \mathbf{z_e}\right) && (4.4) \\ &= \mathbf{H_e^f R s} + \hat{\mathbf{z}}_\mathbf{e}. && (4.5) \end{aligned}$$

In this model, $\mathbf{H_b} \in \mathbb{C}^{[(N+L)\times(N+L)]}$ and $\mathbf{H_e} \in \mathbb{C}^{[(N+L)\times(N+L)]}$ are the Toeplitz matrices corresponding to the channel impulse responses of both Bob and Eve, whereas $\mathbf{H_b^f} = \mathbf{FDH_bCF^H} = \text{diag}[H_{b_1}, \cdots, H_{b_N}] \in \mathbb{C}^{[N\times N]}$, and $\mathbf{H_e^f} = \mathbf{FDH_eCF^H} = \text{diag}[H_{e_1}, \cdots, H_{e_N}] \in \mathbb{C}^{[N\times N]}$ are the diagonal matrices corresponding to the channel frequency responses of Bob and Eve, respectively. Note that H_{b_i} and H_{e_i} for $1 \leq i \leq N$ denote the sub-channel frequency response of the i^{th} sub-carrier with respect to Bob and Eve, respectively. The vectors $\mathbf{z_b}$ and $\mathbf{z_e}$ are formed by the samples of the zero-mean complex additive white Gaussian noise (AWGN) with variances of σ_b^2 and σ_e^2 at Bob and Eve respectively, whilst $\hat{\mathbf{z}}_\mathbf{b}$ and $\hat{\mathbf{z}}_\mathbf{e}$ are the Fourier transformed versions of the noise vectors at Bob and Eve, respectively.

4.3 Proposed Secure OFDM-Subcarrier Index Selection (OFDM-SIS) with Adaptive Interleaving

The key difference between the use of the proposed technique in FDD and TDD modes is the fact that the adaptive interleaver is known to Eve in FDD mode, resulting in one security level, which is provided by the use of optimal subcarrier index selection (SIS). Thus, the proposed scheme is named in FDD mode as

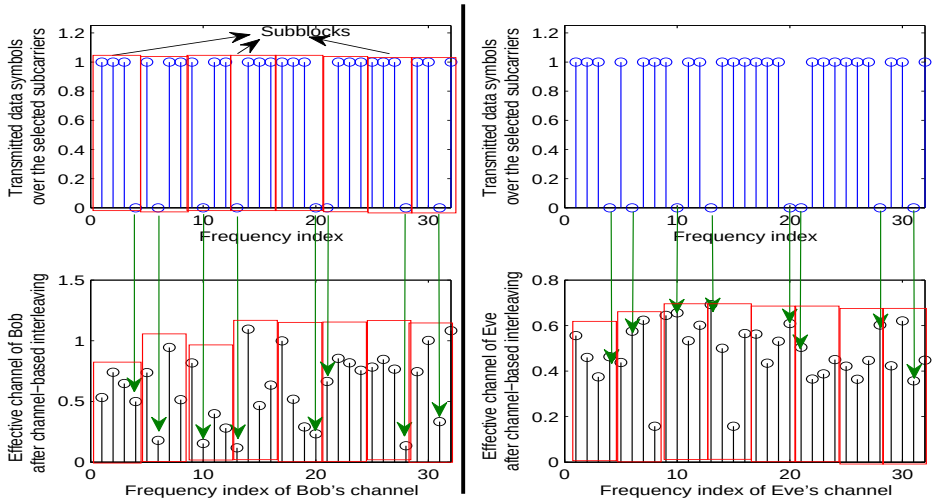


Figure 4.3: Subcarrier structure of the designed secure OFDM-SIS scheme with $\zeta = 3/4$: In each sub-block, surrounded by red rectangle, the sub-carriers experiencing good sub-channel gains with respect to Bob are used for data transmission, while the rest are nulled. Note that with respect to Eve, the nulled sub-carriers do not usually correspond to the weak (bad) sub-channels.

OFDM-SIS. However, in TDD mode, the adaptive interleaver will not be known to Eve, resulting in two security levels which are obtained by both optimal subcarrier index selection and adaptive interleaving (AI). Thus, the scheme is named in TDD mode as OFDM-SIS-AI.

The focus of this section will be on explaining OFDM-SIS, which is introduced for providing secrecy and enhancing reliability. Here, the transmitted OFDM block, i.e., $\mathbf{s}$ of length N, is first divided and partitioned into a set of smaller sub-blocks, each containing K sub-carriers. Recall that interleaving is performed in order to distribute the deep fades of the sub-channels and make them look uncorrelated, random, and uniformly distributed over the whole OFDM block to ensure experiencing a few deep-faded subchannels in each subblock. Also, block partitioning is performed in order to reduce the complexity of the optimization algorithm that will be explained later. The basic idea of the proposed scheme is to enlarge the gap between Bob's and Eve's capacities by making the effective SNR at Bob higher than that at Eve for a given channel frequency response. This is achieved by selecting in each sub-block only the sub-carriers corresponding

to the highest sub-channel gains with respect to the legitimate receiver only. Particularly, for each sub-block, a set of M out of K sub-carriers is optimally selected to maximize the SNR at Bob. Note that the SNR of Bob over each sub-carrier can be given by $SNR_{b_i} = \gamma_b = \frac{P\|H_{b_i}\|^2}{\sigma_b^2}$, where P is the power allocated to each sub-carrier, whereas $\|H_{b_i}\|$ is the subchannel's magnitude. Now, the problem of the optimal selection of indices of M sub-carriers corresponds to solving the below optimization problem for all possible sub-carrier combinations, given as

$$\{c_1^{opt}, \cdots, c_M^{opt}\} = \arg \max_{\{c_1,\cdots,c_M\} \in \mathcal{A}_M} SNR_{b_{[c_1,\cdots,c_M]}}, \tag{4.6}$$

where $\mathcal{A}_M$ denotes the set of all possible subcarrier combinations with M selected out of K sub-carriers, and $SNR_{b_{[c_1,\cdots,c_M]}}$ is the sum of SNRs of the M selected subcarriers in each subblock. In this scheme, we define $\zeta = M/K$ as the sub-carrier activation ratio of the number of selected sub-carriers to the number of available sub-carriers in each sub-block. Now, since uniform power allocation is used for all sub-carriers, the aforementioned problem boils down to selecting the sub-carriers corresponding to the best channel gains. This can be given as below

$$\{c_1^{opt}, c_2^{opt}, \cdots, c_M^{opt}\} = \arg \max_{\{c_1,\cdots,c_M\} \in \mathcal{A}_M} \|H\|_{b_{[c_1,\cdots,c_M]}}, \tag{4.7}$$

where $\|H\|_{b_{[c_1,\cdots,c_M]}}$ is the sum of the magnitudes of the subchannels corresponding to the selected subcarriers. Note that searching all possible subcarrier combinations, i.e., $\binom{K}{M} = \frac{K!}{M!(K-M)!}$, may dictate considerable complexity, especially when the block size is very large. Therefore, it is important to significantly reduce the complexity of solving the above problem. This is achievable when the whole OFDM block is split into smaller parts to reduce the size of the search space.

Moreover, we also want to make sure that, in each sub-block, the sub-carriers have to experience independent as well as different high and low sub-channel gains so that the high ones with respect to Bob can be used for data transmission, while the low ones can be nulled as visualized in Fig. 4.3. It is obvious from Fig. 4.3 that, with respect to Bob, the transmitted data points correspond to high subchannel gains, while the nulled ones correspond to deep-faded sub-channels; on the other hand, the selected subcarriers will correspond to random subchannels with respect to Eve.

To further reduce the complexity of the optimization problem, Alice can select M ($1 \leq M \leq K$) out of K subcarriers that maximizes the effective instantaneous SNR at Bob in each sub-block by first ranking the sub-carriers based on their instantaneous channel gains in a descending order, i.e., $\{\|H_{b1}\|^2 \geq \|H_{b2}\|^2 \geq \cdots \geq \|H_{bK}\|^2\}$. Then, Alice selects the first M indices of the sub-carriers corresponding to the sorted sub-channel gains. It should be noted that this scheme has some similarities with the optimal antenna selection techniques in the spatial domain of MIMO systems [80, 81], but here the selection is performed in the spectral domain of the transmit OFDM waveform and different data symbols are sent over different orthogonal sub-channels.

It is manifest from the aforementioned discussion that two different subcarrier selection procedures are introduced, namely, the combination-based and sorting-based selection schemes. Although we can use any one of them as both are optimal in terms of maximizing the SNR at the legitimate receiver; however, we adopt the sorting-based selection scheme for the rest of the paper due to its low-complexity and low-delay features compared to that of combination-based selection. These features are also very favorable and desirable for URLLC services as well as for compact, battery-limited 5G-IoT devices.

At Bob's side, the captured signal can be given as

$$\mathbf{y_b} = \mathbf{H_b^f R P} \begin{bmatrix} \mathbf{s}_d \\ \mathbf{s}_z \end{bmatrix} + \hat{\mathbf{z}}_\mathbf{b} \in \mathbb{C}^{[N \times 1]}, \tag{4.8}$$

where $\mathbf{s}_d = [s_{(1)}\ s_{(2)}\ \ldots\ s_{(N-N_z)}]^{\mathrm{T}}$ is a vector of $N_d = N - N_z = \zeta N$ frequency data symbols, and $\mathbf{s}_z = [s_{(1)}\ s_{(2)}\ \ldots\ s_{(N_z)}]^{\mathrm{T}}$ is a vector of $N_z = (1-\zeta)N$ nulled sub-carriers. $\mathbf{P}$ is the permutation matrix, which determines the positions (or indices) of the used and nulled sub-carriers in each OFDM block. After discarding the unused nulled sub-carriers, $\mathbf{y_b}$ will have the size of $(\zeta N) \times 1$. Bob then employs the low-complexity zero-forcing frequency domain equalization, followed by deinterleaving, to detect the transmitted data symbols.

At Eve's side, and by assuming that Eve has a sophisticated receiver with full knowledge of the transmission technique and the CSI of the legitimate channel, enabling her to know the indices of the sub-carriers used for data transmission,

its captured signal can be given by

$$\mathbf{y_e} = \mathbf{H_e^f R P} \begin{bmatrix} \mathbf{s}_d \\ \mathbf{s}_z \end{bmatrix} + \hat{\mathbf{z}}_\mathbf{b} \in \mathbb{C}^{[N \times 1]}. \tag{4.9}$$

After discarding the unused nulled sub-carriers, $\mathbf{y_e}$ will have the size of $(\zeta N) \times 1$. For Eve to detect the transmitted symbols, she equalizes its received data symbols vector by its corresponding channel frequency response, and then deinterleaves using $\mathbf{R}$ to detect the transmitted symbols. Note that Eve will not have the same performance as that of the legitimate receiver due to the fact that her channel is different from Bob's one. In other words, since the selected sub-carriers at Alice are independent of Eve's channel, the M strongest, selected transmit sub-carriers for Bob corresponds to a random transmit sub-carriers selection with respect to Eve. According to this design, the proposed OFDM-SIS scheme not only provides secrecy, enhances reliability, and saves power, but also enjoys low-complexity receiver structure compared to the sophisticated ML-based receivers in OFDM-IM.

It is worth mentioning that the proposed scheme results in a controllable spectral efficiency loss due to not using all subcarriers (specifically, the ones with low subchannel gains) for data transmission. However, the adjustable spectral efficiency loss turns into a significant gain in terms of providing better reliability and secrecy with less transmit power and minimal processing and modification at Rx side, making it suitable for URLLC service [73]. Moreover, the extra degree of freedom formed by the OFDM-SIS technique due to subcarrier selection process can provide flexibility in the OFDM design in the sense that it can be exploited to not only enhance secrecy with minimal capacity reduction, but also to perform other useful functionalities. More precisely, unlike OFDM-IM, where the nulled subcarriers cannot be exploited to provide other advantages besides conveying information, in OFDM-SIS, the inactive nulled subcarriers can intelligently be utilized through filling them with specially designed signals to reduce out-of-band emission (OOBE), peak-to-average power ratio (PAPR), and/or adjacent channel interference (ACI) in multiuser scenario as is the case in unique-word OFDM waveform [82]. These kind of designs are beyond the scope of this paper, but can be considered as future works on the proposed technique from the perspective of waveform design.

4.4 Proposed Method for Avoiding Channel Reciprocity Mismatch

Due to the fact that practical wireless TDD systems suffer from having imperfect channel reciprocity (ICR), detrimental side effects can occur when physical layer security techniques are employed due to their channel reciprocity-dependent nature. For instance, channel-based key generation techniques [83] may result in severe BER performance degradation if the generated keys from the channel are not exactly the same at Alice and Bob. To alleviate this problem, several reconciliation methods were proposed in the literature [83] to correct the mismatch that exists in the generated sequences at Alice and Bob. In this process, the mismatch can be removed by the exchange of an information sequence, which is publicly sent through the channel, and thus Eve can easily know part of the generated key. Therefore, privacy amplification is usually used after reconciliation to reduce the amount of leaked information to Eve, but this will decrease the secret key rate. Another issue is that current reconciliation methods are designed to work for sequences of binary random variables, but not matrices of any random variables (as in the case of our proposed secure design). Thus, due to the problems associated with reconciliation and resulted from reciprocity mismatch, in this section, we develop and propose a new practical calibration technique to overcome both the problem of channel reciprocity mismatch (CRM) and the reconciliation-related issues. The proposed technique is inspired by the calibration technique used in 802.11n WiFi standard [84]. However, in the standard the technique was designed without having security in mind, and thus although it can solve the reciprocity problem, it fails to tackle the security problem as the receiver is forced to send publicly a quantized version of the estimated channel to the transmitter. This makes Eve aware of the legitimate user channel, resulting in a security breach as Eve can extract whatever Alice extracts. In the proposed technique, which is summarized in Fig.4.4, channel reciprocity problem is solved without compromising secrecy at all.

Without loss of generality, the basic idea is to let Alice and Bob agree on a

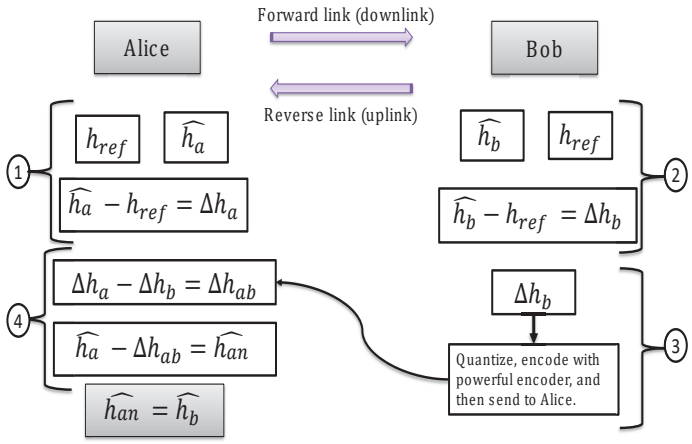


Figure 4.4: Procedure of the proposed method for avoiding channel reciprocity mismatch between Alice and Bob.

reference channel $\mathbf{h_{ref}}$, with which they can compare their channels, and then make use of their differences to compensate the effect of CRM. More precisely, assuming that both Alice and Bob have their estimated erroneous channels (i.e., $\widehat{\mathbf{h_a}}$ and $\widehat{\mathbf{h_b}}$) and a copy of $\mathbf{h_{ref}}$, which can be obtained from a shared random sequence between the legitimate parties [85], then both Alice and Bob can find their channel differences ($\mathbf{\Delta h_a}$ and $\mathbf{\Delta h_b}$) with respect to $\mathbf{h_{ref}}$. Afterwards, Bob quantizes its channel difference $\mathbf{\Delta h_b}$, encodes it using a powerful encoder, and sends it publicly to Alice. Although $\mathbf{\Delta h_b}$ is transmitted publicly, Eve will not be able to get any information about Bob's channel because $\mathbf{\Delta h_b}$ represents the difference between two random unknown sequences. Alice then uses $\mathbf{\Delta h_b}$ to find $\mathbf{\Delta h_{ab}}$ by subtracting $\mathbf{\Delta h_b}$ from $\mathbf{\Delta h_a}$. Finally, Alice subtracts $\mathbf{\Delta h_{ab}}$ from $\widehat{\mathbf{h_a}}$ to get a calibrated channel, denoted as $\widehat{\mathbf{h_{an}}}$, which is exactly equal to Bob's estimated channel $\widehat{\mathbf{h_b}}$. Thus, similar channels at both Alice and Bob are obtained. By utilizing this calibration technique, our proposed security method can be applied reliably without worrying about CRM problem.

4.5 Performance Analysis

Since two levels of security (one by optimal subcarrier index selection and the other by adaptive interleaving) are provided by the proposed security design in the TDD mode, whereas only one security level (optimal subcarrier index selection) is provided in the FDD mode, it is important to quantify the performance obtained by each level individually and then jointly. Thus, in this section, we first analyze the performance obtained by OFDM-SIS (FDD mode), and then by OFDM-SIS-AI (TDD mode).

In order to evaluate the secrecy performance of the proposed OFDM-SIS technique, we need to calculate the statistics of the effective instantaneous SNR at both Bob and Eve, given by $\gamma_b = \frac{\|H_{b_i}\|^2 P}{\sigma_b^2}$ and $\gamma_e = \frac{\|H_{e_i}\|^2 P}{\sigma_e^2}$, respectively. Since both Bob's and Eve's SNRs are functions of the instantaneous amplitude (or power) of their effective corresponding channels, we require to calculate the distributions associated with these quantities so that we can use them to determine the distributions of γ_b and γ_e and then quantify the obtained secrecy and reliability performance.

4.5.1 Statistics of Bob's Effective SNR

The proposed OFDM-SIS results in changing the effective fading distribution over the transmit sub-carriers with respect to Bob. This is due to the fact that a certain percentage of the most deep-faded subchannels are excluded from being used for data transmission, and thus, the fading depth is reduced. The proposed transmission scheme will intuitively lead to an enhancement in the BER performance of the legitimate receiver compared to the standard OFDM transmission as will be demonstrated by computer simulations in Section VI. In order to obtain the distributions of the amplitude and power of the faded subchannels, we use numerical data fitting methods. Particularly, the distributions are obtained by simulating 10000 realizations generated from a standard Rayleigh fading distribution. Then, the proposed OFDM-SIS scheme is applied for selecting the optimal set of sub-carriers, to be used for data transmission. Last, fitting tools

are utilized to find the best matching distribution for the fading amplitude and power of the actual used sub-channels.

It is observed from the fitting results that the effective sub-channel fading amplitude distribution over each sub-carrier under the effect of the proposed technique with $\zeta = 3/4$ turns out to follow Nakagami distribution with shape and scale parameters given by $u = 1.297$ and $w = 1.156$, respectively, as shown in Fig. 4.5. This is different from the conventional OFDM, in which the fading distribution does not change and remains Rayleigh as it is assumed in the system model. Moreover, the effective sub-channel power distribution over each sub-carrier changes from being exponential as is in OFDM to become Gamma with shape and scale parameters given by $u^{'} = 1.297$ and $w^{'} = 0.891$, respectively, as shown in Fig. 4.6. The resulting PDF of the effective sub-channel fading amplitude, i.e., $\alpha = \|H_{b_i}\|$, corresponding to each transmit sub-carrier, can mathematically be given as

$$P_{\alpha}(\alpha) = 2\Big(\frac{u}{w}\Big)^{u} \frac{1}{\Gamma(u)} \alpha^{2u-1} \exp\Big(-\frac{u}{w}\alpha^{2}\Big), \tag{4.10}$$

where u and w are respectively the shape and scale parameters of the obtained Nakagami distribution. Also, we define Ω as the mean square of the sub-channel fading amplitude of α, i.e., $\Omega = E\{\alpha^2\}$. It should be emphasized that the fading distribution of the effective subchannel depends solely on the selection ratio ζ of the proposed scheme. For the two selection ratios we investigate in this paper, i.e., $\zeta = 2/4$ and $\zeta = 3/4$, we have the following Nakagami distribution related parameters:

$$\zeta = 2/4 \Rightarrow u = 1.48, w = 1.31, \Omega = 1.3534 \tag{4.11}$$

$$\zeta = 3/4 \Rightarrow u = 1.297, w = 1.156, \Omega = 1.1565. \tag{4.12}$$

Note that for different values of ζ, different fitting parameters of the Nakagami distribution will be obtained. These are the parameters of the distribution that best fit the effective subchannel amplitude after employing the proposed ODFM-SIS scheme with a certain selection ratio.

Now, the PDF of the effective instantaneous SNR at Bob γ_b can be determined by using a change of variables in the expression for the fading distribution $P_{\alpha}(\alpha)$

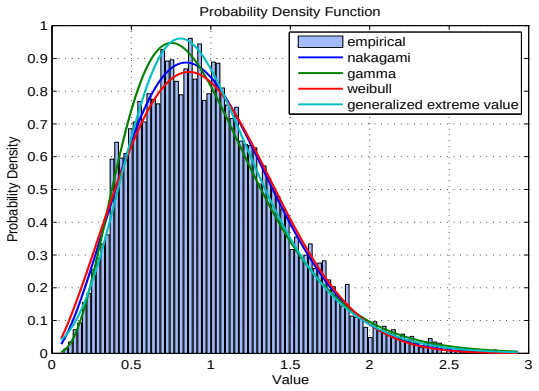


Figure 4.5: The amplitude distribution of the effective subchannels for **Bob** using the proposed technique with $\zeta = 3/4$. As shown, it follows Nakagami distribution with shape and scale parameters given by $u = 1.297$ and $w = 1.156$, respectively. Note that Nakagami fits the best with the aforementioned parameters that are obtained by fitting methods after applying the proposed OFMD-SIS scheme.

of α [86], giving

$$P_{\gamma_b}(\gamma_b) = \frac{P_\alpha\left(\sqrt{\frac{\Omega\gamma_b}{\bar{\gamma_b}}}\right)}{2\sqrt{\frac{\bar{\gamma_b}\gamma_b}{\Omega}}}. \tag{4.13}$$

By considering the special case of $\zeta = 2/4$ as an example and approximating the scale parameter u and make it equal to 1.5, $P_\gamma(\gamma)$ can be given as below[2]

$$P_{\gamma_b}(\gamma_b) \approx \left(\frac{u}{w}\right)^u \frac{1}{\Gamma(u)} \frac{\Omega^{\frac{3}{2}}\sqrt{\gamma_b}}{\bar{\gamma_b}^{\frac{3}{2}}} \exp\left(-\frac{u}{w}\frac{\Omega\gamma_b}{\bar{\gamma_b}}\right). \tag{4.14}$$

The above formula represents a Gamma distribution with parameters associated with $\zeta = 2/4$.

4.5.2 Statistics of Eve's Effective SNR

To find the probability distribution of the instantaneous SNR at Eve under the effect of the proposed technique, we perform fitting for the effective subchannel

[2]The approximation is made in order to be able to integrate the BER formula (to appear in subsection C) and get an *approximated* closed-form expression. Due to this approximation a slight deviation from computer simulation will occur (as it will be shown in Section VI).

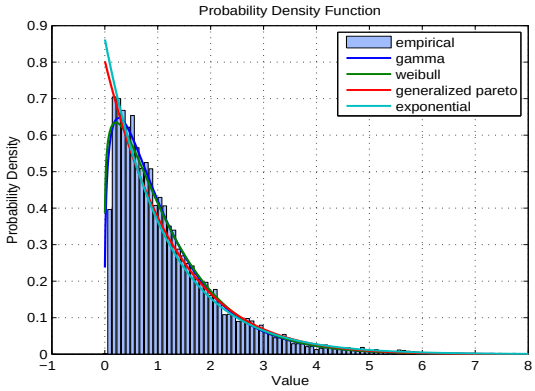


Figure 4.6: The power distribution of the effective subchannels for **Bob** using the proposed technique with $\zeta = 3/4$. As shown, it follows Gamma distribution with shape and scale parameters given by $u^{'} = 1.297$ and $w^{'} = 0.891$, respectively. Note that Gamma fits the best with the aforementioned parameters.

fading amplitude experienced by each transmit sub-carrier similar to the case of Bob's channel. Since selecting the optimal set of subcarriers, corresponding to the strongest set of subchannels for Bob, corresponds to a random subchannels set with respect to Eve, the distribution is intuitively anticipated to be similar to the original assumed fading distribution, i.e., Rayleigh. Our obtained results confirm this intuition and demonstrate that the effective distribution of the subchannel amplitude is approximately Rayleigh distributed (same as the original one) with scale factor β as shown in Fig. 4.7. Also, the effective distribution of the subchannel power is exponential with mean factor ψ as shown in Fig. 4.8. Mathematically, the amplitude subchannel distribution can be given as below:

$$P_{\alpha_e}(\alpha_e) = \frac{\alpha_e}{\beta^2} \exp\left(-\frac{\alpha_e^2}{2\beta^2}\right), \tag{4.15}$$

where β is the scale parameter of the obtained Rayleigh distribution. Also, Ω_e is the mean square variable of α_e i.e., $\Omega_e = E\{\alpha_e^2\}$, which is also equal to ψ obtained by fitting methods. For the selection ratios we adopt in this paper, we have the following approximated distribution parameters

$$\zeta = 2/4 \Rightarrow \beta = 0.706, \Omega_e \approx 1 \tag{4.16}$$

$$\zeta = 3/4 \Rightarrow \beta = 0.704, \Omega_e \approx 1 \tag{4.17}$$

The PDF of γ_e can be determined by using a change of variables in the expression for the fading distribution $P_{\alpha_e}(\alpha_e)$ of α_e, yielding

$$P_{\gamma_e}(\gamma_e) = \frac{P_{\alpha}\left(\sqrt{\frac{\Omega_e \gamma_e}{\bar{\gamma}_e}}\right)}{2\sqrt{\frac{\bar{\gamma}_e \gamma_e}{\Omega_e}}}. \tag{4.18}$$

By taking the special case of the scheme with $\zeta = 2/4$ as an example, the approximated PDF of the effective Eve's SNR, $P_{\gamma_e}(\gamma_e)$, can be given in an exponential distribution form as

$$P_{\gamma_e}(\gamma_e) = \left(\frac{1}{\bar{\gamma}_e}\right) \exp\left(\frac{\gamma_e}{\bar{\gamma}_e}\right). \tag{4.19}$$

Using the above calculated distribution functions, we can now evaluate the BER performance of both Bob and Eve. Moreover, since we now have the SNR statistics of both Bob and Eve, evaluating and analyzing the secrecy performance analytically becomes feasible and convenient, enabling us to examine the advantages of the proposed scheme.

4.5.3 Bob's Average BER

Having formulated the PDF of the instantaneous SNR of Bob, we can analytically evaluate the BER performance of Bob under the effect of the proposed OFDM-SIS scheme. For BPSK/QPSK modulation, the BER of Bob can be given as

$$BER_b = \frac{1}{2}\int_0^{\infty} \operatorname{erfc}(\sqrt{\gamma_b}) P_{\gamma_b}(\gamma_b)\, d\gamma_b, \tag{4.20}$$

where $\operatorname{erfc}(\cdot)$ is the complementary error function. By substituting the PDF of the effective instantaneous SNR of Bob into (20), we get the following integration formula

$$\begin{aligned} BER_b &= \frac{1}{2}\Big(\frac{u}{w}\Big)^u \frac{1}{\Gamma(u)} \frac{\Omega^{\frac{3}{2}}}{\bar{\gamma_b}^{\frac{3}{2}}} \int_0^{\infty} \operatorname{erfc}(\sqrt{\gamma_b})\sqrt{\gamma_b} \\ &\times \exp\left(-\frac{u}{w}\frac{\Omega\gamma_b}{\bar{\gamma_b}}\right) d\gamma_b. \end{aligned} \tag{4.21}$$

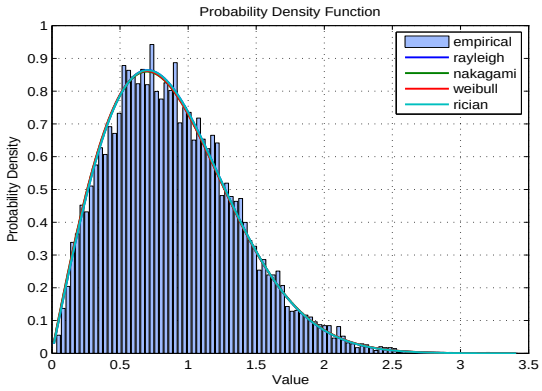


Figure 4.7: The amplitude distribution of the effective subchannels for **Eve** using the proposed technique with $\zeta = 3/4$. As shown, it is Rayleigh distribution with scale parameter $\beta = 0.704$. Note that the other distributions with their own corresponding parameters that make them equivalent to the fitted subchannel power values can also be used in the analysis.

The above integral is solvable [87], and its final solution results in an approximated closed-form expression, which can be given as

$$BER_b \approx \frac{G}{2\sqrt{\pi}} \left(\frac{\arctan\left(\sqrt{\rho}\right)}{2\rho^{3/2}} - \frac{1}{2\rho(1+\rho)} \right), \tag{4.22}$$

where $G = \left(\frac{u}{w}\right)^u \frac{1}{\Gamma(u)} \frac{\Omega^{\frac{3}{2}}}{\bar{\gamma}_b^{\frac{3}{2}}}$, $\rho = \frac{u}{w}\frac{\Omega}{\bar{\gamma}_b}$, and $\arctan(\cdot)$ is the tangent inverse.

It should be mentioned that the above derived BER of Bob is also applicable to the case of TDD mode as optimal subcarrier index selection is used in both modes. Now, since channel coding is not included in the design, adaptive interleaving does not contribute to the BER performance. However, one can expect further enhancement in the BER when coded design is considered as it will improve the decoding performance [79]. It is also important to mention that Bob's BER obviously does not get affected whether Eve knows the interleaver (FDD mode) or not (TDD mode). However, the secrecy level will remarkably be affected as Eve's BER in TDD mode will not be the same due to not knowing the interleaver matrix as it will be shown in the next subsection.

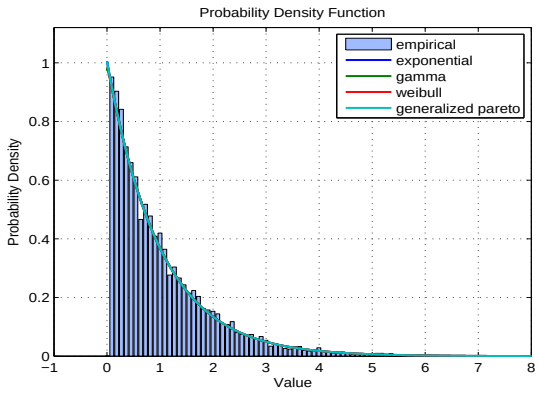


Figure 4.8: The power distribution of the effective subchannels for **Eve** using the proposed technique with $\zeta = 3/4$. As shown, it is exponential distribution with mean parameter $\psi \approx 1$ (which is equal to Ω_e as well). Note that there are four distribution models that match and coincide with each others when considering their own specific fitting parameters.

4.5.4 Eve's Average BER

As we have demonstrated in the previous analysis that the PDF of the instantaneous SNR of Eve does not change and remains Rayleigh as anticipated, one can analytically show that the BER performance of Eve under the effect of the proposed scheme is the same as the conventional OFDM.

For BPSK/QPSK modulation system, the BER of Eve can be given as

$$BER_e = \frac{1}{2}\int_0^{\infty} \operatorname{erfc}(\sqrt{\gamma_e}) P_{\gamma_e}(\gamma_e)\, d\gamma_e. \tag{4.23}$$

By substituting the PDF of the effective instantaneous SNR of Eve into (23), we get the following integration formula

$$BER_e = \frac{1}{2}\int_0^{\infty} \operatorname{erfc}(\sqrt{\gamma_e}) \left(\frac{1}{\bar{\gamma}_e}\right) \exp\left(\frac{\gamma_e}{\bar{\gamma}_e}\right) d\gamma_e. \tag{4.24}$$

The above integral can readily be solved, and its final solution yields an exact closed-form expression for Eve's BER, which can be given as

$$BER_e = \frac{1}{2}\left(1 - \sqrt{\frac{\bar{\gamma}_e}{(1+\bar{\gamma}_e)}}\right). \tag{4.25}$$

For the case of TDD mode, where the adaptive interleaver cannot be known to Eve due to performing the estimation of the legitimate user's channel by using

channel reciprocity-based sounding techniques instead of sending CSI feedback; Eve's BER will not be the same as the above derived formula. Particularly, Eve's BER will severely be affected by her inability to guess the interleaving matrix $\mathbf{R}$.

Since all the subcarrier indices of the OFDM symbol are involved in the interleaving process, there will be $N!$ possible interleaving patterns. Thus, the probability that Eve can guess the extracted interleaver is $P_e = \frac{1}{N!}$. Accordingly, the BER of Eve in TDD mode with unknown interleaving pattern, denoted by BER_e^*, can be given as $BER_e^* \approx P_e \times BER_e + \frac{1}{2}(1 - P_e)$ [69]. It is obvious that the secrecy gap level (i.e., BER difference between Bob and Eve [38]) will significantly be improved as Eve's BER (BER_e^*) will be extremely bad, i.e., Eve's BER will be equal to 0.5, which is the worst random guess any receiver can make.

4.5.5 Secrecy Outage Performance

In this subsection, we use the secrecy outage probability as a metric to analytically evaluate the secrecy performance of the proposed OFDM-SIS scheme in the FDD mode. Secrecy outage is chosen as a suitable metric to quantify the performance because of the fact that the CSI of Eve's channel in a practical passive eavesdropping scenario is neither available to Alice nor to Bob. The secrecy outage probability can be given as [38]

$$P_{\text{sout}} = \Pr\{R_{sec} < R_s\}, \tag{4.26}$$

where R_{sec} is the instantaneous secrecy rate of the proposed OFDM-SIS technique and is given by $R_{sec} = [R_b - R_e]^+$, in which $[q]^+$ denotes $\max\{0; x\}$, $R_b = \log_2(1+\gamma_b)$ is the instantaneous rate of the Bob's effective channel, and $R_e = \log_2(1+\gamma_e)$ is the instantaneous rate of the Eve's effective channel, whereas $R_s > 0$ is a predefined targeted secrecy rate. The secrecy outage probability can be further defined as [6]

$$\begin{aligned} P_{\text{sout}} &= \Pr[R_{sec} < R_s \mid \gamma_b > \gamma_e] \Pr[\gamma_b > \gamma_e] \\ &+ \Pr[R_{sec} < R_s \mid \gamma_b \leq \gamma_e] \Pr[\gamma_b \leq \gamma_e]. \end{aligned} \tag{4.27}$$

Since $\Pr[R_{sec} < R_s \mid \gamma_b \leq \gamma_e]$ always equals to unity when $\gamma_b \leq \gamma_e$, the above formula can be reduced to

$$\begin{aligned} P_{\text{sout}} &= \Pr[R_{sec} < R_s \mid \gamma_b > \gamma_e] \Pr[\gamma_b > \gamma_e] \\ &+ \Pr[\gamma_b \leq \gamma_e]. \end{aligned} \tag{4.28}$$

Using probability concepts, we can rewrite the previous formula as

$$P_{\text{sout}} = \int_0^\infty F_{\gamma_b}\left(2^{R_s}(1+x)-1\right) f_{\gamma_e}(x)dx, \tag{4.29}$$

where x stands for the realizations of γ_e due to notational simplicity (i.e., $f_{\gamma_e}(x) = P_{\gamma_e}(\gamma_e)$). $F_{\gamma_b}(.)$ is the CDF of the SNR of Bob. For $\zeta = 2/4$, the CDF of γ_b can be obtained by integrating its PDF given in (14), resulting in the following expression

$$F_{\gamma_b}(x) = G\left(\frac{\sqrt{\pi}\,\text{erf}\left(\sqrt{\rho}\sqrt{x}\right)}{2\rho^{\frac{3}{2}}} - \frac{\sqrt{x}\text{e}^{-\rho x}}{\rho}\right), \tag{4.30}$$

where erf(.) is the error function [87]. By substituting the CDF and PDF of the effective instantaneous SNR of Bob and Eve, respectively, into (29), we get the following formula for P_{sout}

$$\begin{aligned} &= rG\int_0^\infty \left(\frac{\sqrt{\pi}\,\text{erf}\left(\sqrt{\rho}\sqrt{(2^{R_s}(1+x)-1)}\right)}{2\rho^{\frac{3}{2}}}\text{e}^{-rx}dx\right) \\ &- rG\int_0^\infty \left(\frac{\sqrt{(2^{R_s}(1+x)-1)}\text{e}^{-\rho\left(2^{R_s}(1+x)-1\right)}}{\rho}\text{e}^{-rx}\right)dx \end{aligned} \tag{4.31}$$

where $r = \frac{1}{\bar{\gamma}_e}$. By integrating the above equation, we obtain the final expression of the secrecy outage probability formula given in (32), which is placed in the top of next page, where $\Gamma(.,.)$ is the incomplete Gamma function [87].

4.6 Simulation Results

In this section, we provide computer simulation results to demonstrate and validate the effectiveness of the proposed security scheme and to also examine the

$$
\begin{aligned}
P_{\text{sout}} &= \left[\frac{rG\sqrt{\pi}}{2\rho^{\frac{3}{2}}} \left(\frac{\sqrt{\rho}\cdot 2^{\frac{R_s}{2}} \mathrm{e}^{r-\frac{r}{2^{R_s}}} \operatorname{erf}\left(\frac{\sqrt{\rho\cdot 2^{R_s}+r}\sqrt{2^{R_s}x+2^{R_s}-1}}{2^{\frac{R_s}{2}}} \right)}{r\sqrt{\rho\cdot 2^{R_s}+r}} - \frac{\mathrm{e}^{-rx} \operatorname{erf}\left(\sqrt{\rho}\sqrt{2^{R_s}x+2^{R_s}-1}\right)}{r} \right) \right. \\
&+ \left. \left[\frac{rG\,\Gamma\left(\frac{3}{2}, \frac{\left(\rho\cdot 2^{R_s}+r\right)\left(2^{R_s}x+2^{R_s}-1\right)}{2^{R_s}}\right) \rho^{\frac{3}{2}}\cdot 2^{\frac{R_s}{2}+1} \mathrm{e}^{\frac{r\left(2^{R_s}-1\right)}{2^{R_s}}}}{\rho\left(\rho\cdot 2^{R_s}+r\right)^{\frac{3}{2}}} \right]_0^{\infty} \right. . \\
&= \frac{rG\sqrt{\pi}}{2\rho^{\frac{3}{2}}} \left(\frac{\sqrt{\rho}\cdot 2^{\frac{R_s}{2}} \mathrm{e}^{r-\frac{r}{2^{R_s}}}}{r\sqrt{\rho\cdot 2^{R_s}+r}} - \frac{\sqrt{\rho}\cdot 2^{\frac{R_s}{2}} \mathrm{e}^{r-\frac{r}{2^{R_s}}} \operatorname{erf}\left(\frac{\sqrt{\rho\cdot 2^{R_s}+r}\sqrt{2^{R_s}-1}}{2^{\frac{R_s}{2}}} \right)}{r\sqrt{\rho\cdot 2^{R_s}+r}} + \frac{\operatorname{erf}\left(\sqrt{\rho}\sqrt{2^{R_s}-1}\right)}{r} \right) \\
&- \frac{rG\,\Gamma\left(\frac{3}{2}, \frac{\left(\rho\cdot 2^{R_s}+r\right)\left(2^{R_s}-1\right)}{2^{R_s}}\right) \rho^{\frac{3}{2}}\cdot 2^{\frac{R_s}{2}+1} \mathrm{e}^{\frac{r\left(2^{R_s}-1\right)}{2^{R_s}}}}{\rho\left(\rho\cdot 2^{R_s}+r\right)^{\frac{3}{2}}}. \qquad (4
\end{aligned}
$$

impacts of the selection ratio and the average SNR on the security and reliability performance. First, we quantify the secrecy performance obtained by OFDM-SIS scheme in an FDD mode, then we examine the expected performance gain when OFDM-SIS-AI is used in a TDD mode. We consider a practical uncoded SISO-OFDM system with $N = 64$ sub-carriers adopting quadrature phase shift keying (QPSK) modulation and a guard period of length L. The number of sub-blocks in each OFDM block is considered to be $N/K = 16$, where each sub-block contains $K = 4$ available sub-carriers. Two different values of the activation ratio ζ are considered, i.e., $\zeta = 3/4$ and $\zeta = 2/4$. The channel is modeled as an independent and identically distributed (i.i.d.) block-fading, where channel coefficients are drawn from a Rayleigh fading distribution, and the channel is deemed to be slowly varying. The Rayleigh multi-path fading channels of both Bob and Eve are assumed to have the same length, $L = 9$ samples, with a normalized power delay profile given by $\mathbf{p} = [0.8407,\ 0,\ 0,\ 0.1332,\ 0,\ 0.0168,\ 0.0067,\ 0,\ 0.0027]$ mW [88]. Additionally, we consider an eavesdropper, who perfectly knows the transmission technique used at Alice as well as the CSI of the legitimate receiver in an FDD system during the channel feedback process.

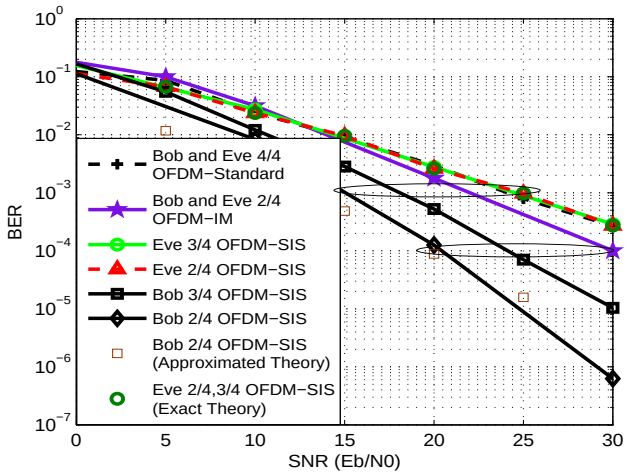


Figure 4.9: BER of both Bob and Eve using the proposed OFDM-SIS in FDD mode compared to OFDM and OFDM-IM. QPSK modulation and different ζ values are used. FDD system is considered, where Eve knows Bob's CSI.

In the performance evaluation, we use both secrecy outage probability metric to quantify the achievable secrecy level, and BER-based secrecy gap metric [52] to not only evaluate the secrecy, but also to quantify the amount of information leakage to Eve and the reliability enhancement with respect to the legitimate receiver.

Fig. 4.9 shows the BER performance gain of a legitimate Rx, employing the proposed OFDM-SIS in FDD mode with selection ratios $\zeta = 3/4$ and $\zeta = 2/4$ compared to an OFDM-IM scheme with unity and half selection ratios, i.e., $\zeta = 4/4 = 1$ and $\zeta = 2/4 = 0.5$, respectively. Note that OFDM-IM with unity selection ratio corresponds to standard OFDM. Particularity, it is shown that OFDM-SIS outperforms OFDM at BER=10^{-3} by more than 5 dB and by around 10 dB for $\zeta = 3/4$ and $\zeta = 2/4$, respectively, and the gain difference gradually grows as the SNR increases. This gain is obtained by utilizing the optimal sub-carrier selection scheme according to the Bob's channel, in such a way that the Bob's SNR is maximized. This causes avoiding the deep-faded sub-channels (which limits the performance) with respect to only Bob, resulting in changing the fading distribution to a less severe fading, and thus, enhancing the BER performance of the fading-limited OFDM-based transmission waveforms.

Generally, it is observed from Fig. 4.9 that the BER performance enhances

as the selection ratio decreases with the price of reduced spectral efficiency. More precisely, an extra gain of 5 dB is achieved at BER= 10^{-4} when the selection ratio reduced from $\zeta = 3/4$ to $\zeta = 2/4$. It should be mentioned that for $\zeta = 2/4$, the slight mismatch between the derived closed form BER expression of Bob and its numerical result is due to two reasons: 1) the necessary approximation we used for the scale parameter u, which appears in the PDF of the effective SNR of Bob, as stated in the footnote of Section IV; 2) the effective subchannel amplitude distributions of Bob over each subcarrier changes according to the considered power-delay profile of the channel. Specifically, it is observed that the channel amplitude fading distribution in OFDM-SIS is not exactly the same for all subchannels as opposed to the case in conventional OFDM.

Furthermore, Fig. 4.9 exhibits the BER performance of Eve assuming that she is fully aware of the used scheme and also the interleaving matrix as well as the indices of the sub-carriers selected for data transmission as she is considered to know the legitimate CSI link in case of FDD system. Both simulation and analytical results exhibit matching BER performance and prove that Eve's BER under the proposed scheme is the same as that of standard OFDM as expected. This happens due to the use of channel-dependent optimal subcarrier indices selection with respect to Alice-to-Bob channel that is different from Alice-to-Eve channel, for which the selection process looks random (not optimal). Thus, the system response will not be favorable to Eve and no performance gain is delivered to her.

It is also observed that Eve's BER does not change with the variation of selection ratio and the secrecy gap between Bob's and Eve's sides increases as the average SNR grows due to the enhancement in the Bob's BER. The obtained secrecy gap is significant and can be utilized to provide QoS-based secrecy [33], [38]. For instance, at BER= 10^{-4}, there is a difference (secrecy gap) of 10-12 dB between Bob and Eve, and thus for a service requiring BER below 10^{-4}, Bob can reliably use the service when his average SNR is equal or greater than 20 dB, while Eve is prevented from using it at comparable SNR values. In fact, Eve needs 10-12 dB more signal power than the average SNR of Bob (i.e., Eve's SNR must be at least 32 dB) to be able to decode the same service reliably. This

created gap in BER performances between Bob and Eve results in a good secrecy level that can be effectively utilized to deliver a certain service securely.

Fig. 4.10 depicts the performance of the secrecy outage probability achieved by the introduced OFDM-SIS scheme in FDD mode when the predefined secrecy rate threshold is set to unity (i.e., $R_s = 1$). Secrecy outage is drawn versus Bob's average SNR when Eve's average SNR ($\bar{\gamma}_e$) is equal to 0 dB and 10 dB, while the selection ratio ζ equals to 2/4, 3/4, and 4/4. From Fig. 4.10, we see that the decrease of ζ results in a better secrecy outage performance as the effective SNR at Bob increases. This occurs due to avoiding deep fades and using only the subchannels of highest gain with respect to Bob.

Fig. 4.11 presents the secrecy gap performance obtained by OFDM-SIS-AI, which is used in TDD mode and provides two security levels: one by the adaptive interleaver and the other by the subcarrier index selection. This figure also provides the comparison of the OFDM-SIS-AI scheme with OFDM-SIS, which is proposed for the FDD mode and also used in TDD mode. Particularly, Fig. 4.11 shows that the BER performance of Eve using OFDM-SIS-AI remains at 0.5 for both selection ratios $\zeta = 2/4$ and $\zeta = 3/4$ as Eve has no information about the interleaver matrix extracted from Bob's channel. Also, the BER of Bob is the same as that provided by the OFDM-SIS scheme in an uncoded system for the same ζ values. It is important to mention that OFDM-SIS-AI scheme can provide better BER performance to the legitimate user when channel coding is used as it breaks burst errors by mitigating the correlation between subchannels, and thus enhancing the decoding capability. Note that the performance investigation of the proposed scheme with channel coding as well as the effect of practical issues, such as synchronization and estimation errors are beyond the scope of this paper, and left for future research studies.

Based on the obtained results and from both security and reliability perspectives, we have demonstrated that the reliability performance of the proposed OFDM-SIS scheme outperforms both conventional OFDM as well as OFDM-IM. Furthermore, the secrecy performance gain is achieved not only in TDD mode, but also in FDD mode by considering a very challenging scenario where Eve can access the CSI of the legitimate link, and without sharing secret keys, or knowing Eve's channel, or even causing any major changes in the receiver design. Given

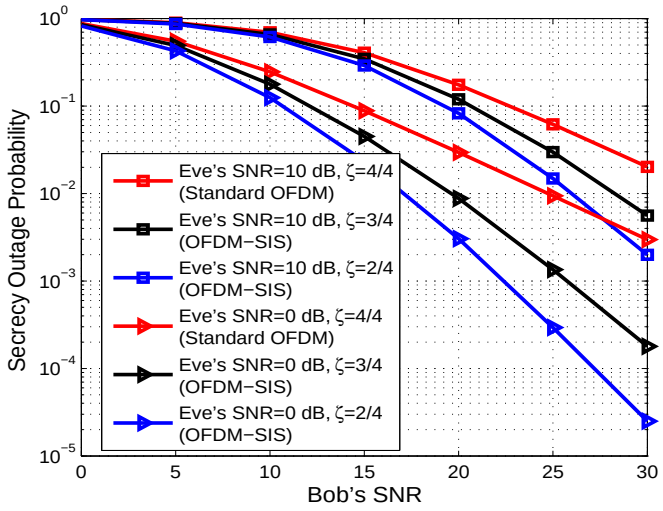


Figure 4.10: Secrecy outage probability of the proposed OFDM-SIS in FDD mode for $\zeta = 1, 0.75, 0.5$; $R_s = 1$; and $\bar{\gamma}_e = 0$ dB and 10 dB.

the simplicity of the proposed design, its hardware testbed implementation is very handy and straightforward to build, making it very appealing for advanced 5G and beyond systems and URLLC services as well as low-complexity Internet of Things (IoT) devices.

It is noteworthy to mention that there is an interesting trade-off between the achievable secrecy and reliability from one side and spectral efficiency from another side (i.e., both secrecy and reliability performance enhances as the spectral efficiency decreases). This trade-off is fully controllable and adjustable via the selection ratio parameter ζ, which can be modified according to the requirements of the user applications and services.

Moreover, the proposed scheme has the advantage of the new degree of freedom created from the selection process, which can provide more flexibility in the OFDM design. More precisely, the subcarriers that are not used for data transmission because of their low subchannel gains, which already limit the performance of both BER and throughput, can be deliberately filled with specially designed signals, that can perform other important functionalities like reducing OOBE and PAPR in each subblock for burst transmission scenarios [66]. In this kind of design, better secrecy and reliability can be achieved while mitigating the

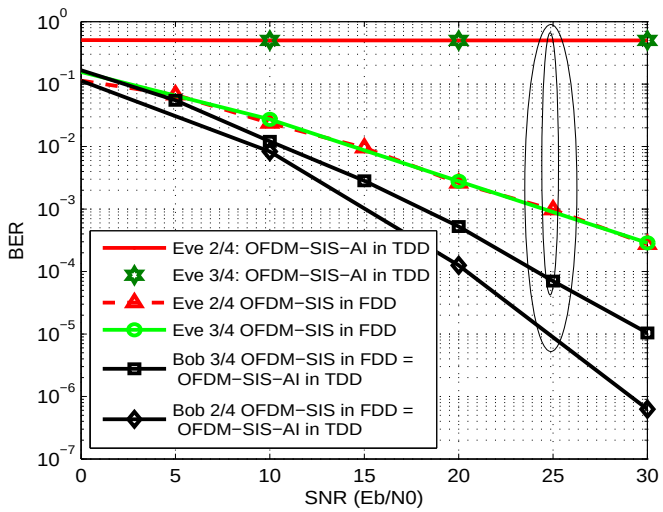


Figure 4.11: BER secrecy gap comparison between the proposed OFDM-SIS in FDD mode and OFDM-SIS-AI in TDD mode. QPSK modulation with different ζ values are used.

effect of challenging problems such as power leakage, PAPR, and interference. Thus, there is almost no loss in the overall system performance, but rather more gains.

It should also be emphasized that although OFDM-SIS is proposed in this work for a single user scenario, where the subcarriers assigned to a certain user are channel-dependent as well as adaptively distributed over the whole band (with a structure similar to that of OFDM-IM before interleaving) thanks to the use of channel-based adaptive interleavers; OFDM-SIS can also be employed for multi-user scenarios. Specifically, in a multi-user scenario, full subcarrier utilization can be achieved as bad subcarriers with respect to a certain user can be good with respect to another user experiencing a different channel condition. Thus, minimal spectral efficiency reduction of the proposed scheme can be guaranteed by assigning the nulled subcarriers with respect to a certain user to other users in the network to send their data over these subcarriers, which may experience good subchannel gains, resulting in what is called *multi-user diversity* facilitated by different scheduling and resource allocation techniques.

4.7 Conclusion

An efficient 5G URLLC-tailored physical layer security technique, which can provide two security levels in TDD mode and one in FDD mode, has been proposed for protecting OFDM-based waveforms against eavesdropping. In this technique, named as OFDM-SIS, the frequency response of correlated subchannels is first converted into a completely uncorrelated effective response by means of adaptive channel-based interleaving. Then, the whole OFDM symbol is divided into small sub-blocks, each containing a set of sub-carriers experiencing uncorrelated random sub-channels, from which we select and use only the ones corresponding to good sub-channels for data transmission, while the remaining ones are suppressed. This transmission mechanism results not only in providing remarkable secrecy gap, but also enhances the reliability performance of the legitimate user compared to the standard OFDM transmission. Moreover, the technique saves power and provides secrecy even in the worst security scenario, where the eavesdropper is assumed to know the channel of the legitimate link due to using some kind of explicit FDD-based feedback. The presented results have proven the capability of the proposed scheme in achieving practical secrecy without increasing the complexity of the OFDM structure or knowing Eve's channel, making it very suitable for low complexity 5G-URLLC services (IoT-based remote control and tactile applications). Future work can consider designing and investigating the secrecy performance of different variations of the proposed OFDM-SIS scheme assuming different block sizes and activation ratios. Moreover, utilizing the degree of freedom created by the proposed scheme for providing larger secrecy gap as well as performing other advantageous functionalities besides secrecy, such as reducing PAPR and mitigating OOB leakage (two main drawbacks of OFDM-based waveforms) is an appealing future research direction in order to maximize the overall system performance gain.

Chapter 5

CP-Less OFDM with Alignment Signals for Enhancing Spectral Efficiency, Reducing Latency, and Improving PHY Security of 5G and Beyond Services

5.1 Introduction

Due to its numerous advantages, orthogonal frequency devision multiplexing (OFDM) [89] has been the most dominantly used transmission waveform in the vast majority of the currently available standards, such as WiFi, WiMax, DVB, LTE, and NB-IoT. Moreover, it should not be a surprise that OFDM waveform (with its new parametrized waveforms to meet the diverse requirements of different emerging applications) is expected to maintain its dominance in future 5G systems [66, 90, 91]. It has been adopted due to its desirable features, including higher spectral efficiency, robustness to multipath with simple equalization in the frequency domain, easy integration with MIMO systems, and multi-user diversity

where time and frequency resources are flexibly scheduled among users based on their requirements and channel conditions [90].

Nonetheless, OFDM has several major drawbacks, such as high peak-to-average power ratio (PAPR), spectral leakage, strict synchronization requirements and frequency offset sensitivity. These issues have been heavily studied in the literature and many solutions were proposed to mitigate their side effects [90, 92, 93]. Besides the aforementioned issues, there are other issues which have not been studied much in the literature, but have started gaining the attention of researchers due to their significant importance for future dynamic, low latency, spectral and power efficient 5G wireless networks. Among these issues are the ones related to the non-optimal design of OFDM, which can be summarized in two aspects: 1) the excessive usage of cyclic prefix (CP) as guard times between OFDM symbols to prevent inter-symbol-interference (ISI) while providing circular convolution; and 2) the inability to optimally collect and effectively combine the leaked energy (due to channel dispersion) of the OFDM symbol to the guard time owing to the fixed waveforms length of OFDM transceiver structure.

For the issue of collecting the energy leakage, the authors in [52, 94] designed a new waveform that can optimally collect the dispersive signal energy that leaks to the guard time part of the signal instead of just discarding it as is the case in standard OFDM. The designed waveform in [52], which is named as orthogonal transform division multiplexing (OTDM), results in a better reliability compared to standard OFDM due to accumulating the dispersive energy and combining it optimally with the data symbols. Also, the design yields physical layer secrecy [95] as an extra advantage that comes for free due to making the waveform channel-dependent.

On the other hand, the issue of using excessive CPs between OFDM symbols makes OFDM suffer from a significant spectral efficiency loss as well as latency increase due to using a fraction of the available time resources as guard intervals instead of utilizing them for data transmission. This motivates designing new novel solutions that can completely release and free the need for using CPs between OFDM symbols while maintaining good reliability performance as that of

the standard CP-OFDM. This issue is substantially important and worth to be practically solved as it causes a huge waste of resources in some specific emerging 5G scenarios and services such as massive machine type communication (mMTC) and enhanced mobile broadband (eMBB) [96], resulting in an inability to enhance the total efficiency and transmission rate of the wireless systems. Besides, CP also causes extra unnecessary transmission delay for latency-sensitive applications such as ultra reliable and low latency communication (URLLC) services [66, 96].

To realize the significant effect of this issue and how much important it is to properly address this issue, we give the following explanatory example. In mMTC scenarios [97], massive amount of Internet of Things (IoT) devices often receive and transmit sporadic short packets of control and sensed data to 5G base station (BS) whose resources are usually limited and may become insufficient when the BS tries to serve all these massive devices simultaneously. Let us assume we have 10000 of these IoT devices, each requires on average 100 OFDM symbols of 512 sub-carrier resources. With current standard OFDM waveform, where the CP length can be as large as one fourth (0.25) of the whole OFDM symbol, the BS would sacrifice around $10000\times100\times0.25\times512$=128,000,000 units of time resources. This is an extremely huge amount of loss in the total spectral efficiency of just one BS as these resources could be saved and then used to serve other users and IoT devices in the network.

Moreover, mitigating the CP length (denoted by R) or totally removing it will certainly help meet the requirements of enhanced mobile broadband (eMBB) services that not only require high spectral efficiency but also low transmission latency (a very desirable feature for URLLC services as well) to increase peak throughput. Particularly, latency can significantly be reduced if the net OFDM symbol duration is made equal to only the useful data part of the symbol (i.e., data subcarriers N) instead of being equal to the sum of data and guard time parts. Consequently, in low latency applications, the CP becomes a considerable overhead which not only degrades the system spectral efficiency by $N/(N+R)$, but also causes latency and energy efficiency loss. Motivated by these practical facts, it would be extremely very advantageous if one could develop practical methods that can totally remove the need for inserting CPs between OFDM

symbols while maintaining the same performance as that of standard OFDM.

In the literature, there are several techniques introduced to mitigate the spectral efficiency loss and latency due to CP by either reducing (shorting) or totally removing (eliminating) the CP guard period while maintaining reasonable performance. Among the techniques used to reduce the required guard time are channel shortening schemes that are capable of reducing the CP length by either utilizing a time-domain equalizer to shorten the effective channel impulse response as in [98], or frequency-domain equalizer as in [99], or by designing proper precoding matrices as in [100] and [101]. Besides channel shortening, in [102], authors proposed an asymmetric window which provides a significant CP reduction without increasing out-of-band-emission (OOBE) nor causing ISI/ICI. In [103], authors explored a scheme based on the concept of multiple symbol encapsulation, which was originally introduced in [104] to reduce CP rate. The authors of [103] showed that the scheme can noticeably mitigate the CP overhead and hence increase the throughput by using only a single CP to a group (block) of adjacent OFDM symbols instead of inserting many CPs between consecutive OFDM symbols in each transmission block. At the receiver, a frequency domain equalization technique that applies FFT and IFFT on the whole block was proposed for cancellation of any ISI/ICI resulting from multipath channels.

All the aforementioned techniques can be classified under the category of CP-short approach. On the other hand, there are other techniques that can be classified under the category of CP-free approach. These CP-free OFDM techniques aim to totally remove the CP guard times, and hence achieving the maximum gain in terms of higher spectral efficiency and lower latency. In [105], a Nyquist pulse shaping filter bank was utilized to OFDM for CP elimination. In [106], a CP-free OFDM transmission scheme, called overlapping based OFDM (Ov-OFDM), was proposed to shorten the total OFDM symbol length without guard overhead. The scheme utilizes an overlapping minimum mean square error (MMSE) frequency domain equalization to eliminate ISI between OFDM symbols. In [107], a low-complexity frequency-domain equalizer that utilizes redundancy in the frequency domain was proposed to completely suppress ISI and ICI when no guard intervals

are inserted between symbols. In [108], a different equalizer based on a multi-antenna generalized side-lobe canceler (GSC) was also proposed to suppress ISI for high-rate SIMO-OFDM systems without CP. The method basically depends on the block representation of the OFDM transmission and exploits the subspace of the ISI structure in the multi-antenna scenarios. In [109], authors introduced a non-orthogonal and CP-free scheme based on maximum-likelihood sequence detection in frequency domain to enhance spectrum and power efficiency from one side and alleviate synchronization requirement from another side. The detection algorithm is termed as frequency-domain maximum-likelihood sequence detection (MLSD). In [110], a multi-carrier detection algorithm for OFDM systems without guard time by utilizing successive interference cancellation with decision feedback was also introduced. Most recently, the authors of [39] proposed a scheme called symbol cyclic shift equalization (SCSE) to implement a CP-free OFDM system. The scheme is based on performing decision feedback equalization (DFE) before FFT operation for removing the ISI between the overlapped OFDM symbols. The scheme also uses CP restoration mechanism at the receiver to convert linear shift into circular shift, thereby allowing the use of FFT transform at the receiver. Despite its effectiveness, this scheme comes with three major demerits. First, it results in an excessive, unaffordable complexity at the receiver[1], making it unsuitable for low complexity, battery-limited devices (such as IoT). Second, it makes the design incompatible with current and future expected devices, where minimal or even no changes in the receiver terminal are required to reduce to cost of making new reception designs. Third, its bit-error rate performance is worse than that of OFDM for certain channel types. Due to these issues, SCSE appears to be not a very good fit for future 5G services and specifically for mMTC applications with massive IoT devices, which are expected to be compact in size, light in processing, and limited in battery power consumption.

As inferred from the literature, most of the proposed CP-free and CP-short approaches are based on either utilizing equalization technologies such as MMSE,

[1]Note that the authors in [111] tried to reduce the complexity of SCSE scheme by using pulse amplitude modulation (PAM) instead of M-ary quadrature amplitude modulation (M-QAM). This unfortunately can not be applied to current and future systems that mainly adopt M-QAM.

ZF, DFE, SIC and so forth; or exploiting some redundancy in the spectral or spatial domain to mitigate or eliminate CP overhead at the expense of extra complexity at the receiver or wasting other resources.

In this paper, we propose **a novel power domain based-scheme, called CP-less OFDM,** that removes the requirement of inserting CP between successive OFDM symbols, while keeping the whole detection process the same at the receiver side without the need to use any complex equalizers. This is achieved by adding an alignment signal on top (in the power domain) of each transmitted OFDM symbol to guarantee achieving two goals simultaneously: 1) canceling the interference of one symbol on the other adjacent one, and 2) maintaining the circularity property of the received signals before the low complexity frequency domain equalization process. The obtained results demonstrate the superiority of the proposed CP-less OFDM scheme in terms of spectral efficiency, reduced latency, power efficiency, and physical layer secrecy compared to standard CP-OFDM while maintaining low complexity using simple one tap frequency domain equalizer, making the design inherently compatible with current and future systems, and also highly capable of meeting the needs of 5G and beyond wireless services.

The main advantages of the proposed scheme can be emphasized and summarized as follows:

- Enhancing spectral efficiency and throughput due to removing the time resources required by CP.
- Enhancing power efficiency as a result of saving the power consumed by CP, where the power of the alignment signal in our proposed design is less than that of CP in OFDM.
- Reducing transmission latency due to decreasing the net time duration required for the transmission of each symbol.
- Improving physical layer security [52, 95] as a consequence of making the alignment signal function of the legitimate user's channel, which is different from that of eavesdroppers located at different locations. Thus, extra

interference will be caused to the eavesdroppers.

- The scheme does not require any changes or extra processing at the receiver thanks to the proper design of the added alignment signal, making it compatible with current and future networks. In particular, all the processing is done at the transmitter, making it very suitable for the downlink transmission scenario (from BS to low complexity IoT devices).

A highly critical and **emerging 5G scenario** that our proposed CP-less OFDM method is particularly suited for is URLLC type of services. This is so due to the fact that the OFDM symbol durations in URLLC services are required to be much smaller compared to the symbol durations currently being used in 4G and WiFi systems in order to provide low latency and much faster communication. However, this increases the CP overhead for a given fixed channel delay spread if conventional CP-OFDM scheme is used. Therefore, removing the CP requirement with the proposed method can result in a highly efficient transmission system. Our scheme can even become more beneficial for the scenarios of stationary channels (e.g., access point communicating with a non-moving wireless terminal) where the receiver in this case does not require to frequently send pilot signals to the transmitter to update the channel estimation process at the transmitter as the channel is almost static (i.e., not varying much).

These highly desirable merits are achieved at the **expense** of a slight increase in the processing complexity at the base station alongside the need for acquiring channel state information (CSI) at the transmitter [52, 62, 112–114].

The rest of the chapter is organized as follows. The system preliminaries and assumptions are described in Section 5.2. The details of the devised CP-less OFDM waveform by using two different methods are revealed in Section 5.3. Numerical results including BER, spectral efficiency, transmission latency, power saving, secrecy performance, robustness to imperfect channel, PAPR, OOBE, complexity; are all presented, discussed and explained in Section 5.4, which is followed by conclusion and future works in Section 5.5.[2]

[2] *Notations*: Vectors are denoted by bold-small letters, whereas matrices are denoted by

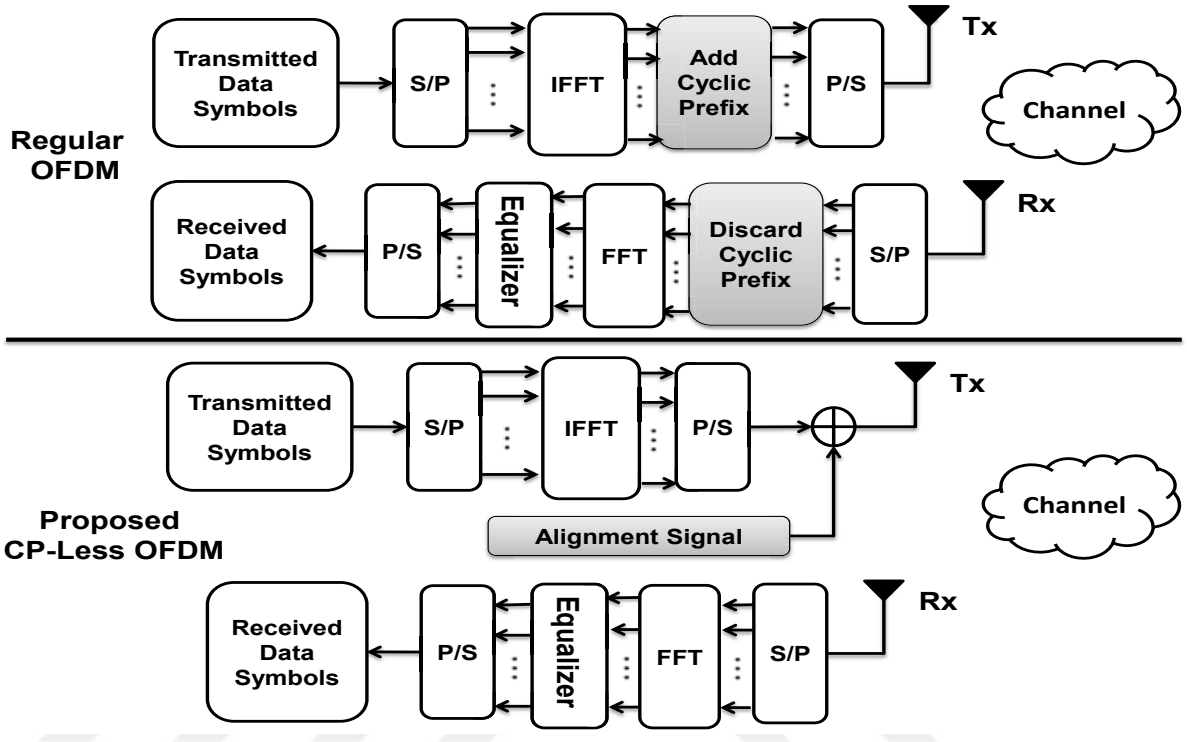


Figure 5.1: Transceiver structures of the conventional, regular OFDM and the proposed CP-less OFDM.

5.2 Preliminaries and Assumptions

A regular single-input single-output (SISO) OFDM system as depicted in the upper part of Fig. 5.1 is considered as a reference baseband system model upon which we develop our proposed scheme. In the regular OFDM system, the M-ary modulated frequency data symbols are first converted from serial to parallel and then passed through an IFFT block, resulting in a time domain signal vector, whose samples are coming from the contribution of all the frequency data symbols. Then, a CP of length equal to or greater than the channel spread length is appended to the time domain signal to avert ISI and provide channel circularity. The signal is then sent serially from the transmitter (Tx) to the receiver (Rx) over a multi-path frequency selective and slowly varying fading channel denoted

bold-large letters. The convolution operator is indicated by $(*)$. The transpose, hermitian (conjugate transpose) and inverse are symbolized by $(\cdot)^T$, $(\cdot)^H$ and $(\cdot)^{-1}$, respectively. $\mathbf{I}$ is the $N \times N$ identity matrix.

by $\mathbf{h} = \begin{bmatrix} h_0 & h_1 & ... & h_R \end{bmatrix}^T \in \mathbb{C}^{[(R+1)\times 1]}$, where $(R+1)$ is the number of taps. The channel impulse response has $R+1$ taps, each experiences Rayleigh fading distribution. At the Rx side, the received samples are first converted from serial to parallel, and then the CP is cut and discarded. Afterwards, the samples are passed through an FFT block, followed by one tap frequency domain channel equalization to recover the M-ary modulated frequency data symbols.

Unlike the aforementioned described classical OFDM design, in the proposed CP-less OFDM scheme as portrayed in the lower part of Fig. 5.1, there is neither CP addition at the Tx nor CP removal at the Rx. Instead, a well-designed alignment signal (AS) is added on top of the time domain CP-free OFDM symbol in order to both cancel the ISI caused between adjacent OFDM symbols due to channel dispersion, and convert linear convolution into circular one so that low complexity frequency domain equalization can be used instead of the extremely complex time domain equalization [39].

In this work, the channel reciprocity property is adopted, where the downlink channel can be estimated from the uplink one in a time division duplexing (TDD) or hybrid systems (TDD with FDD) [62]. The channel realizations are assumed to be known at the transmitter [53,62] so that a special AS can be properly designed to enhance the spectral efficiency and reduce latency (with low complexity) of the system by eliminating the need for inserting CPs between successive OFDM symbols.

For the secrecy performance evaluation, we also consider an eavesdropper, called Eve, who tries to intercept the communication between the legitimate Tx and Rx parties, called Alice and Bob, respectively. Eve also experiences a multipath channel of independent realizations from the one experienced by the legitimate receiver as the channel de-correlates for different locations that are distant from each other by half-wave length or more [52, 62, 95].

5.3 Proposed CP-Less OFDM Design

The key concept underlying the transmission mechanism of the proposed CP-less OFDM with AS, whose transceiver structure is briefly illustrated in the lower part of Fig. 5.1, is clearly visualized in Fig. 5.2. As exhibited, a specially designed AS (colored in red) is superimposed with the OFDM time domain signal (colored in gray) in the power domain at the Tx side. After passing through the channel and reaching the Rx side, the AS accumulates itself and aligns over the interference part of the OFDM signal to cancel ISI and provide circularity. In this section, we provide the mathematical and physical meaning details of the proposed scheme at both the Tx and Rx sides.

At the Tx, the total number of frequency data symbols to be sent is N, where each transmitted OFDM block is represented as $\mathbf{x} = \begin{bmatrix} x_0 & x_1 & ... & x_{N-1} \end{bmatrix}^T \in \mathbb{C}^{[N\times 1]}$. Each OFDM block $\mathbf{x}$ is then passed through an IFFT process $\mathbf{F}^{\mathrm{H}} \in \mathbb{C}^{[N\times N]}$, which basically maps the frequency data points to orthogonal sub-carriers, where $\mathbf{F}$ is the discrete Fourier transform matrix. Thus, the time domain samples of each OFDM symbol can be given as $\mathbf{s} = \mathbf{F}^{\mathrm{H}}\mathbf{x}$. At this point, no CP addition is used, instead, a specially designed alignment signal (AS) of size equal to $N \times 1$ and denoted by $\mathbf{c} = \begin{bmatrix} c_0 & c_1 & ... & c_{N-1} \end{bmatrix}^T \in \mathbb{C}^{[N\times 1]}$ is added on top of each CP-less OFDM signal. In other words, the AS is superimposed to the power domain of the time domain signal of the original CP-less OFDM symbol. Thus, the total resulting i^{th} CP-less OFDM signal to be transmitted can be modeled as

$$\mathbf{t_i} \;\; = \;\; \mathbf{s_i} + \mathbf{c_i} = \mathbf{F}^{\mathrm{H}}\mathbf{x_i} + \mathbf{c_i} \in \mathbb{C}^{[N\times 1]}. \tag{5.1}$$

Now, the key idea behind the proposed design is based on the fact that each added AS [112, 113] at the Tx can be designed to perfectly align to a specific target part of the OFDM symbol after passing through the channel and reaching at the receiver side as shown in Fig. 5.2. Since the AS can be aligned at any specific part, it would be beneficial to align the AS to the dispersive part (due to which we need CP in standard OFDM) of the OFDM signal and try to design the value of the AS in such away that can cancel the interference that appears in that specific part of the signal. Note that the length of the dispersive part (i.e.,

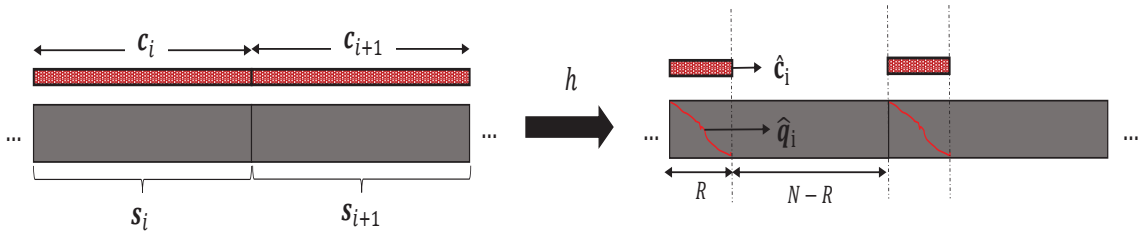


Figure 5.2: Visualization of the designed CP-less OFDM with alignment signal superposition for two consecutive OFDM symbols.

the region of ISI) of OFDM symbol is equal to the number of channel samples, which is denoted by R. Additionally, in order to have the same functionality as that provided by CP in standard CP OFDM, an aligned AS at the receiver, $\hat{\mathbf{c}}_\mathbf{i} \in \mathbb{C}^{[R\times 1]}$, should correspond to the summation of both an interference canceling signal $\hat{\mathbf{q}}_\mathbf{i} \in \mathbb{C}^{[R\times 1]}$ to compensate the ISI between successive OFDM symbols and a circularity providing signal $\hat{\mathbf{z}}_\mathbf{i} \in \mathbb{C}^{[R\times 1]}$ to maintain circularity and have simple one tap frequency domain equalization without the need to use complex time domain equalizers. Let us assume a channel impulse response of $R+1$ taps with exponentially decaying function. These taps are first estimated using channel sounding techniques [114] and then used to construct a Toeplitz matrix of size $N+R$ by N (to be used for calculating the value of the alignment signal). Then, the interference term on i^{th} signal can be calculated as

$$\hat{\mathbf{q}}_\mathbf{i} \;=\; \mathbf{H_p}\mathbf{t_{i-1}} \in \mathbb{C}^{[R\times 1]}, \tag{5.2}$$

where $\mathbf{t_{i-1}}$ is the previously transmitted CP-less OFDM symbol and $\mathbf{H_p} \in \mathbb{C}^{[R\times N]}$ is the dispersive channel part, which can be given as

$$\mathbf{H_p} \;=\; \begin{bmatrix} 0 & \cdots & h_R & \cdots & h_0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & h_R \end{bmatrix}. \tag{5.3}$$

Note that $\mathbf{H_p}$ represents the interference part of the Toeplitz matrix of the channel impulse response with $R+1$ taps for a block-based transmission system. More precisely, $\mathbf{H_p}$, which is basically the last R rows of the channel Toeplitz matrix, causes dispersion and inter-symbol-interference between OFDM blocks when CP is not used. The Toeplitz matrix is denoted by $\mathbf{H} \in \mathbb{C}^{[(N+R)\times N]}$, and can be given

as

$$\mathbf{H} = \begin{bmatrix} \mathbf{H_u} \\ \mathbf{H_p} \end{bmatrix} = \begin{bmatrix} h_0 & 0 & \cdots & \cdots & 0 \\ \vdots & h_0 & 0 & \ddots & \vdots \\ \vdots & \vdots & h_0 & \ddots & \vdots \\ h_R & \vdots & \vdots & \ddots & 0 \\ 0 & h_R & \vdots & \ddots & h_0 \\ \vdots & 0 & h_R & \ddots & \vdots \\ \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & \cdots & h_R \end{bmatrix}, \tag{5.4}$$

where $\mathbf{H_u}$ is the interference-free channel convolution matrix (i.e., $\mathbf{H}$ without the dispersion-responsible part represented by the last R rows).

On the other hand, the circularity providing signal for the i^{th} signal can be obtained as

$$\hat{\mathbf{z}}_\mathbf{i} = \mathbf{H_p s_i} \in \mathbb{C}^{[R\times 1]}. \tag{5.5}$$

Then, $\hat{\mathbf{c}}_\mathbf{i}$ which is the required signal at the receiver for interference cancellation and circularity assurance can be given as

$$\hat{\mathbf{c}}_\mathbf{i} = \hat{\mathbf{z}}_\mathbf{i} - \hat{\mathbf{q}}_\mathbf{i} = \mathbf{H_p s_i} - \mathbf{H_p t_{i-1}} \in \mathbb{C}^{[R\times 1]}, \tag{5.6}$$

which can further be simplified into the below form

$$\hat{\mathbf{c}}_\mathbf{i} = \mathbf{H_p}\left(\mathbf{s_i} - \mathbf{s_{i-1}} - \mathbf{c_{i-1}}\right) \in \mathbb{C}^{[R\times 1]}. \tag{5.7}$$

In order to design such an AS, we firstly need to find the null space of the multiplication of the interference-free channel convolution matrix (i.e., $\mathbf{H_u}$) and an imaginary CP removal matrix that creates nulls at the beginning of each OFDM symbol. Now, the real valued, virtual CP removal matrix is defined as if it removes the first R samples of each transmission symbol. Let us give that as $\mathbf{B} \in \mathbb{C}^{[(N-R)\times N]}$. Then the required null space can be calculated as

$$\mathbf{P} = \ker\left(\mathbf{B H_u}\right) \in \mathbb{C}^{[N\times R]}, \tag{5.8}$$

where ker( ) corresponds to kernel extracting operation, by which we can find the null space of the effective channel matrix $\mathbf{BH_u}$ so that we can use this null space to align the added AS into the specific part of the OFDM symbol. Note that any vector $\mathbf{w_i} \in \mathbb{C}^{[R\times 1]}$ multiplied by $\mathbf{P}$ and passed through the channel will give an AS aligning on the first R samples of the OFDM symbol. Note that this AS also leaks to the next symbol but we consider that as interference and will be canceled by the next symbol's AS. Therefore, the AS at the transmitter can be calculated as

$$\mathbf{c_i} \;=\; \mathbf{P w_i} \in \mathbb{C}^{[N\times 1]}. \tag{5.9}$$

By doing so, we guarantee the alignment of the added AS in the desired portion of the OFDM signal at the receiver side. In the next step, we will calculate the values of $\mathbf{w_i}$ in order to obtain the desired signal, $\hat{\mathbf{c}}_\mathbf{i}$.

The i^{th} received baseband signal can be given as

$$\mathbf{y_i} \;=\; \mathbf{h} * \mathbf{t_i} + \mathbf{n_i} = \mathbf{h} * (\mathbf{s_i} + \mathbf{c_i}) + \mathbf{n_i} \in \mathbb{C}^{[(N+R)\times 1]}, \tag{5.10}$$

where $\mathbf{y} = \begin{bmatrix} y_0 & y_1 & \dots & y_{N+R} \end{bmatrix}^T$, in which $y_i = \sum_{l=0}^{R} h_l t_{(i-l)} + n_{(i)}$, and $\mathbf{n_i} \in \mathbb{C}^{[(N+R)\times 1]}$ is the zero-mean complex additive white Gaussian noise (AWGN) at the Rx. The above convolution form can also be rewritten in a matrix form as

$$\mathbf{y_i} = \mathbf{H t_i} + \mathbf{n_i} = \mathbf{H}(\mathbf{s_i} + \mathbf{c_i}) + \mathbf{n_i}. \tag{5.11}$$

The net received signal including the interference coming from the previous symbol can be given as

$$\mathbf{y_i} \;=\; \underbrace{\mathbf{H s_i}}_{\text{Desired signal plus interference}} + \underbrace{\mathbf{H c_i}}_{\text{Alignment signal}} + \underbrace{\hat{\mathbf{H}}_\mathbf{p} \mathbf{t_{i-1}}}_{\text{Interference signal}} + \mathbf{n_i}, \tag{5.12}$$

where $\hat{\mathbf{H}}_\mathbf{p}$ can be given as

$$\hat{\mathbf{H}}_\mathbf{p} = \begin{bmatrix} \mathbf{H_p}^{[R\times N]} \\ \mathbf{0}^{[N\times N]} \end{bmatrix}. \tag{5.13}$$

In order to achieve a CP free transmission, the second term of $\mathbf{y_i}$, $\mathbf{Hc_i} = \hat{\mathbf{c}}_\mathbf{i}$ should be $\hat{\mathbf{H}}_\mathbf{p}\left(\mathbf{s_i} - \mathbf{t_{i-1}}\right)$ as mentioned before. We can interpret $\hat{\mathbf{c}}_\mathbf{i}$ as a column vector whose first R elements cancel ISI and introduce circularity, and the other N elements are supposed to be perfectly zero. The second term of $\mathbf{y_i}$ can be given as

$$\hat{\mathbf{c}}_\mathbf{i} = \mathbf{Hc_i} = \mathbf{HPw_i}. \tag{5.14}$$

It can be seen that the last N elements of $\hat{\mathbf{c}}_\mathbf{i}$ will be zero. Then, we can focus the multiplication of $\mathbf{HPw_i}$ which should give us the required values as the first R elements of $\hat{\mathbf{c}}_\mathbf{i}$. Thus, $\mathbf{w_i}$ can readily be calculated as

$$\begin{aligned} \mathbf{w_i} &= \left(\mathbf{HP}\right)^{-1}\hat{\mathbf{c}}_\mathbf{i} && (5.15)\\ &= \left(\left(\mathbf{HP}\right)^{H}\left(\mathbf{HP}\right)\right)^{-1}\left(\mathbf{HP}\right)^{H}\hat{\mathbf{c}}_\mathbf{i}. && (5.16) \end{aligned}$$

By the time the properly designed AS passes through the channel and reaches the Rx, the ISI will be naturally canceled by the added AS. Thus, the received N interference-free samples of the effective OFDM symbol along with the circularity-providing signal component, can be given as

$$\mathbf{y_i} = \mathbf{H_u s_i} + \begin{bmatrix}\mathbf{H_p}\\ \mathbf{0}\end{bmatrix}\mathbf{s_i} + \hat{\mathbf{n}}_\mathbf{i} \in \mathbb{C}^{[N\times 1]}, \tag{5.17}$$

where $\hat{\mathbf{n}}_\mathbf{i}$ has the first N samples of the original vector $\mathbf{n_i}$. One can see that the above effective received OFDM symbol can be written in terms of a circular channel matrix denoted by $\mathbf{H_c} \in \mathbb{C}^{[N\times N]}$ as follows

$$\mathbf{y_i} = \mathbf{H_c s_i} + \hat{\mathbf{n}}_\mathbf{i} \in \mathbb{C}^{[N\times 1]}. \tag{5.18}$$

Afterwards, the Rx applies fast Fourier transform by using the matrix $\mathbf{F}$ to get the frequency data symbols of each OFDM symbol, which can be given as

$$\begin{aligned} \hat{\mathbf{y}}_\mathbf{i} &= \mathbf{FH_c s_i} + \mathbf{F}\hat{\mathbf{n}}_\mathbf{i}\\ &= \mathbf{FH_c F^H x_i} + \mathbf{F}\hat{\mathbf{n}}_\mathbf{i}\\ &= \mathbf{H_f x_i} + \mathbf{F}\hat{\mathbf{n}}_\mathbf{i}. && (5.19) \end{aligned}$$

Lastly, the Rx uses the diagonal channel frequency response $\mathbf{H_f} = diag\begin{bmatrix}H_0 & H_1 & ... & H_N\end{bmatrix}$ to perform simple one tap zero-forcing equalization process on $\hat{\mathbf{y}}_\mathbf{i}$ to get the final equalized data symbols block $\hat{\mathbf{x}}$, which can be given

as

$$\begin{aligned} \hat{\mathbf{x}}_\mathbf{i} &= \mathbf{H}_\mathbf{f}^{-\mathbf{1}}\mathbf{H}_\mathbf{f}\mathbf{x}_\mathbf{i} + \mathbf{H}_\mathbf{f}^{-\mathbf{1}}\mathbf{F}\hat{\mathbf{n}}_\mathbf{i} \\ &= \mathbf{x}_\mathbf{i} + \mathbf{H}_\mathbf{f}^{-\mathbf{1}}\mathbf{F}\hat{\mathbf{n}}_\mathbf{i}. \end{aligned} \tag{5.20}$$

It should be mentioned that the previous proposed design is based on the concept of CP-OFDM, which is the most commonly used OFDM scheme in wireless systems. In the following, we present an alternative design inspired by the concept of zero padding (ZP)-OFDM with overlap addition (OLA) receiver structure. This second proposed design inspired by ZP is equivalent to the first proposed design inspired by CP in the sense that both of them have the same system performance. The key difference between the two designs (methods) is that, in the aforementioned presented CP-inspired design, the added AS tries to cancel the interference coming from its proceeding adjacent symbol; whereas in the design inspired by ZP-OFDM with OLA, the AS tries to cancel the interference caused by each symbol onto its later adjacent symbol. Thus, instead of making the AS function of both the current and previous symbols as presented before, in this new alternative design, the AS will be function of only the current symbol.

Without loss of generality, in this second proposed method, one can design two signals, namely, an interference-canceling signal $\mathbf{u_i}$ to cancel the ISI caused by each i^{th} OFDM symbol onto the other right-adjacent symbol given be $\hat{\mathbf{u}}_\mathbf{i}$, and a circularity-providing signal for the i^{th} symbol $\mathbf{z}_i$ to convert linear convolution to circular one at the receiver $\hat{\mathbf{z}}_\mathbf{i}$, thereby enabling the use of simple one tap frequency domain equalization by performing FFT operation. Particularly, the ISI signal at the end of each OFDM symbol at the receiver can mathematically be given as

$$\hat{\mathbf{u}}_\mathbf{i} = \mathbf{H}_\mathbf{p}\mathbf{s}_\mathbf{i} \in \mathbb{C}^{[R\times 1]}, \tag{5.21}$$

whereas the circularity providing signal at the beginning of each OFDM symbol at the receiver can be given as

$$\hat{\mathbf{z}}_\mathbf{i} = \mathbf{H}_\mathbf{p}\mathbf{s}_\mathbf{i} \in \mathbb{C}^{[R\times 1]}, \tag{5.22}$$

According, the alignment signal that should be added at the transmitter to cancel ISI can be given as

$$\mathbf{H}\mathbf{u_i} = \begin{bmatrix} \mathbf{0}^{[N\times 1]} \\ -\hat{\mathbf{u}}_\mathbf{i}^{[R\times 1]} \end{bmatrix} \tag{5.23}$$

$$\mathbf{u_i} = \left((\mathbf{H})^H (\mathbf{H})\right)^{-1} (\mathbf{H})^H \begin{bmatrix} \mathbf{0}^{[N\times 1]} \\ -\hat{\mathbf{u}}_\mathbf{i}^{[R\times 1]} \end{bmatrix}, \tag{5.24}$$

whereas the alignment signal that should be added at the transmitter to provide circularity can be calculated as

$$\mathbf{H}\mathbf{z_i} = \begin{bmatrix} \hat{\mathbf{z}}_\mathbf{i}^{[R\times 1]} \\ \mathbf{0}^{[N\times 1]} \end{bmatrix} \tag{5.25}$$

$$\mathbf{z_i} = \left((\mathbf{H})^H (\mathbf{H})\right)^{-1} (\mathbf{H})^H \begin{bmatrix} \hat{\mathbf{z}}_\mathbf{i}^{[R\times 1]} \\ \mathbf{0}^{[N\times 1]} \end{bmatrix}. \tag{5.26}$$

Thus, the total resulting i^{th} signal to be transmitted can be modeled and calculated as

$$\mathbf{t_i} = \mathbf{s_i} + \mathbf{u_i} + \mathbf{z_i} \in \mathbb{C}^{[N\times 1]} \tag{5.27}$$

$$= \mathbf{F}^{\mathrm{H}}\mathbf{x_i} + \left((\mathbf{H})^H (\mathbf{H})\right)^{-1} (\mathbf{H})^H \begin{bmatrix} \mathbf{0}^{[N\times 1]} \\ -\hat{\mathbf{u}}_\mathbf{i}^{[R\times 1]} \end{bmatrix} + \left((\mathbf{H})^H (\mathbf{H})\right)^{-1} (\mathbf{H})^H \begin{bmatrix} \hat{\mathbf{z}}_\mathbf{i}^{[R\times 1]} \\ \mathbf{0}^{[N\times 1]} \end{bmatrix} \tag{5.28}$$

It is worth mentioning that the merits of the proposed design are not limited to just enhancing spectral efficiency and reducing latency without introducing any extra or complex processing at the Rx side, but also in providing physical layer security against eavesdropping [56], which is a very desirable merit of the proposed scheme for future inherently secure services and IoT applications. Secrecy can be provided because the AS is designed to be a function of the intended user channel, which is usually different from that of the eavesdropper [52]. Thus, investigating and quantifying the exact secrecy performance of the proposed scheme and its coexistence with other schemes and layers can be a subject of future research as it is beyond the main scope of this paper.

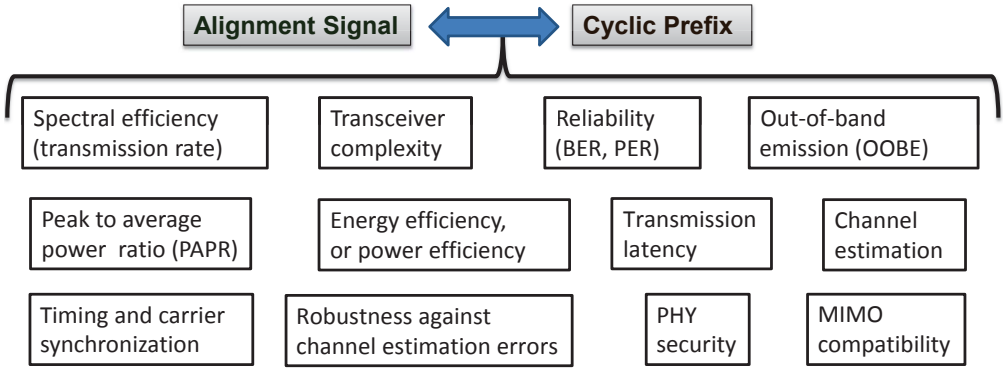


Figure 5.3: Different performance aspects and measures that can be investigated for providing thorough and comprehensive comparison between CP-less OFDM featured by AS and regular OFDM featured by CP.

5.4 Performance Evaluation Results and Discussion

In this section, we present the performance results of the proposed CP-less OFDM compared to regular CP OFDM. Particularly, we use transmission efficiency (bps/Hz), transmission latency (time samples), and power efficiency as main performance metrics to validate and demonstrate the gain that can be achieved by the proposed CP-less OFDM compared to CP OFDM. Moreover; BER, PAPR, and OOBE metrics are also evaluated to investigate the effect of the proposed design on these performance metrics under various conditions. A comprehensive picture of the performance aspects and measures that can be investigated for providing thorough and comprehensive comparison between CP-less OFDM featured by AS and regular OFDM featured by CP can be seen in Fig. 5.3. To achieve this inclusive investigation, we perform computer simulations for an OFDM signal having N=64 subcarriers and modulation is determined as QAM with M=4 (unless otherwise stated). The number of OFDM symbols in each frame is assumed to be 20.

The power delay profile of the adopted Rayleigh multipath time dispersive channel is defined to be an exponentially decaying with (R+1) taps and expressed

as

$$h(DF, n) = ae^{-DF \times n}; n = 0, 1, \cdots, CDS \times N. \tag{5.29}$$

where a is the normalization factor, n represents the tap index, and DF is the decaying factor of the channel which is set to have the following values: DF=1, DF=2, and DF=3. Also, CDS is defined as the channel delay spread length of the channel with respect to the OFDM symbol length (N). In this setup, CDS is configured to take the following values[3]: CDS=1/8, CDS=1/4, and CDS=1/2 (unless otherwise stated). The channel is assumed to be changing from one frame to another independently and perfect channel estimation is assumed [52,112,113].

5.4.1 Bit Error Rate (BER)

The bit-error-rate (BER) comparison of a regular CP OFDM signal and proposed CP-less OFDM (or CP-free OFDM) signal is given in Fig. 5.4. As obviously seen, the proposed CP-less OFDM technique, which totally removes the redundancy of CP, exhibits BER performance close to that provided by regular OFDM as the decaying factor of the channel increases, while a slight degradation, resulting in an error floor occurs as the decaying factor of the channel decreases.

After deep investigation and exploration of the reason behind this performance behavior that makes BER affected by the decaying factor of the channel (although the theory provided by the mathematical design in Section 3 shows that we can completely cancel the interference), we found out that it is generally impossible to accurately find the inverse of the term $\left(\left(\mathbf{HP}\right)^H \left(\mathbf{HP}\right)\right)^{-1}$, which appears in the equation of calculating the alignment signal given as

$$\mathbf{w_i} = \left(\left(\mathbf{HP}\right)^H \left(\mathbf{HP}\right)\right)^{-1} \left(\mathbf{HP}\right)^H \hat{\mathbf{c}}_\mathbf{i}. \tag{5.30}$$

Computing the accurate precise inverse is impossible in some cases where the channel matrix is overdetermined with low decaying factors (i.e., tall matrix with

[3] CDS=1/8 means that the length of the channel spread when N=64 is equal to $1/8 \times 64 = 8$ samples.

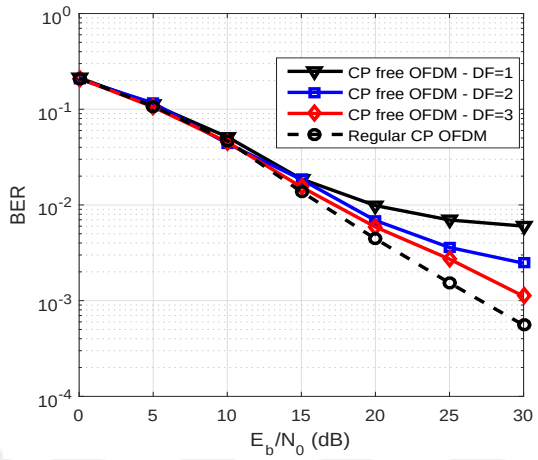


Figure 5.4: BER comparison between CP-less OFDM and CP OFDM with different channel decaying factors when the channel spread length is equal to one forth of the OFDM symbol period. QPSK modulation and N=64 subcarriers are used.

more rows than columns and a few eigenvalues approaching zero). Consequently, the added alignment signal will not be effective in such cases and will not do its assumed job, which is to cancel the interference and provide circularity. In this case, since the added alignment signal will not be able to perfectly cancel the interference, a certain amount of performance degradation is anticipated. To avoid this degradation, we can measure the length of the interference in terms of time samples and then add a CP of length equal to that of the interference. Another way to avoid this interference is to use decision feedback equalization (DFE) with CP restoration algorithm as proposed in [39]. Besides the aforementioned reason related to matrix inverse, it is also observed that the use of MATLAB pseudo inverse function for overdetermined matrices (which is the case in our design $\mathbf{H}$) results in a noticeable sensitive inaccuracy. This happens as the pseudo-inverse function has a certain level of tolerance that must be used in order to be able to find an approximate pseudo-inverse that is usually calculated using a least square

estimate[4] since an accurate result is impossible. This inherent mathematical difficulty results in a slight interference when the channel decaying factor is small, yielding a slight BER degradation as shown in Fig. 5.4 of the BER performance. To overcome such a difficultly, more accurate and advanced mathematical tools for calculating the inverse with higher accuracy and lower tolerance error are needed to be investigated in future research studies.

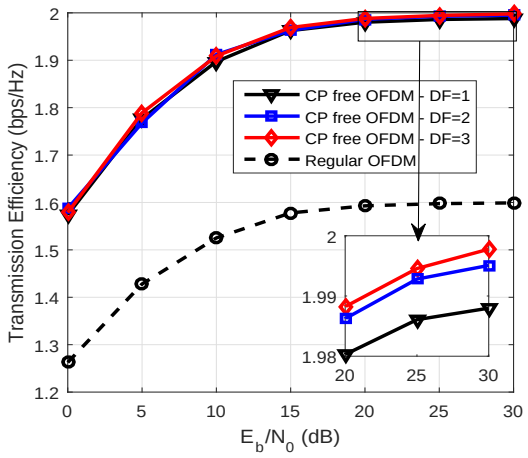


Figure 5.5: Transmission efficiency comparison between CP-less OFDM and CP OFDM with different channel decaying factors when the channel spread length is equal to one forth (1/4) of the OFDM symbol period, QPSK modulation is used, and N=64.

[4]It should be mentioned that the calculation of approximate pseudo-inverse using least square estimate yields a certain level of complexity at the transmitting BS at the benefit of having minimal equalization complexity at the receiving IoT device. This complexity at BS can be affordable due to having higher processing power capabilities at the BS compared to that available at IoT devices, which have constraints on the power and processing capabilities. For this reason, the proposed CP-less OFDM scheme is best suitable to be implemented in the downlink scenarios (transmission from BS to IoT device). Thus, similar to LTE standard, the frame structure of uplink will use SC-FDMA (SC-FDE), whereas downlink will adopt CP-less OFDM instead of CP-OFDM.

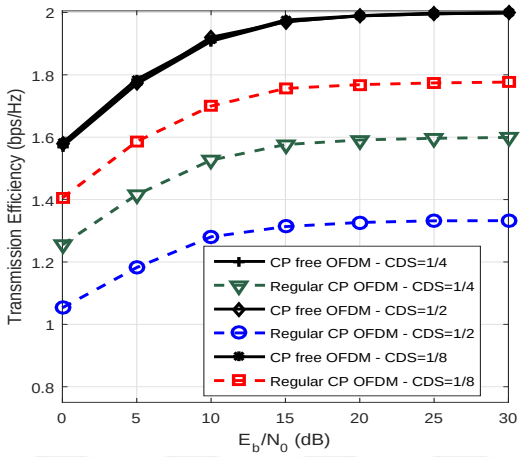


Figure 5.6: Transmission efficiency comparison between CP-less OFDM and CP OFDM with different channel delay spread lengths, when QPSK modulation is used, DF=1, and N=64.

5.4.2 Transmission Efficiency

Fig. 5.5 shows the superiority of the transmission efficiency[5] of the proposed CP-free OFDM design compared to CP OFDM where the CP length is set to be equal to the channel delay spread (i.e., 16 samples, which is the one fourth of the whole OFDM symbol length). It is clear from Fig. 5.5 that around 0.4 bps/Hz transmission efficiency gain as a result of using the proposed CP-less OFDM compared to regular OFDM. Note that the maximum spectral efficiency that can be achieved at high SNR values can be calculated according to the below formula that takes CP length into account

$$\eta = \frac{\log_2 M \times N}{(N + R)}, \tag{5.31}$$

where for the case of CP-less OFDM, R is always equal to zero as there is no CP overhead, whereas for the case of CP OFDM, R is equal to the channel delay spread of the channel at minimal.

Fig. 5.6 is plotted to compare the transmission efficiency between CP-less OFDM and regular OFDM when different channel delay spread (CDS) values

[5]The transmission efficiency is calculated in the same manner as done in the literature of CP-free OFDM design [39] [111].

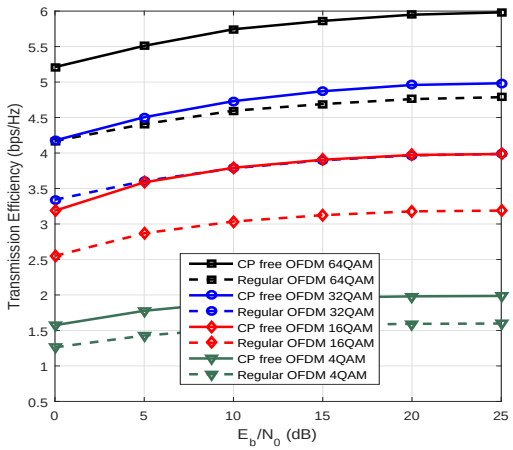


Figure 5.7: Transmission efficiency comparison between CP-less OFDM and CP OFDM with different modulation orders when the channel spread length is one forth of the OFDM symbol period.

are used. It is shown that the maximum achievable transmission efficiency values of regular OFDM are 1.35, 1.6, and 1.8 for CDS values of 1/2, 1/4, and 1/8, respectively. On the other hand, the transmission efficiency of CP-less OFDM is shown to be independent of the CDS and always reaches its maximum value at high SNR, which is equal to 2 bps/Hz when QPSK is used. This clearly demonstrates the fact that the spectral efficiency gain difference between CP-less OFDM and CP OFDM increases as the channel delay spread becomes longer. It should be mentioned that the gain in transmission efficiency is achieved at the cost of extra processing at the transmitter alongside the need to use accurate channel estimators with robust calibration techniques [114]. The validity of the received data is directly related to the reliability of the received data, which is measured by average BER metric as shown in Fig. 5.4.

Fig. 5.7 sketches the maximum achievable transmission efficiency versus SNR of the proposed scheme compared to regular OFDM under the effect of different modulation orders when the CDS is set to be 1/4. It is evident that there are gains of 1.2, 1, 0.8, and 0.4 for modulation types of 64QAM, 32QAM, 16QAM, and 4QAM, respectively. This states that the gain difference enhances as the modulation order increases.

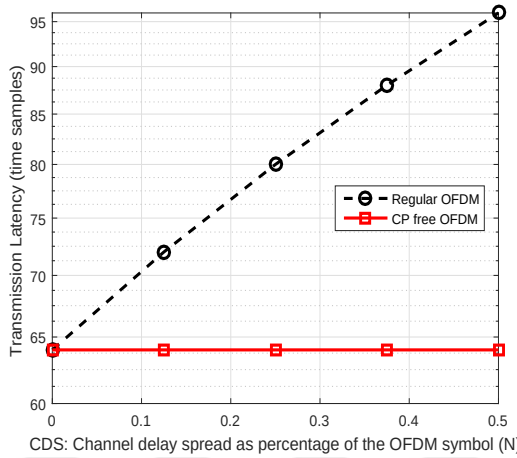


Figure 5.8: Transmission latency comparison between CP-less OFDM and CP OFDM versus channel delay spread length.

5.4.3 Transmission Latency

One of key merits of the proposed CP-less OFDM scheme is that it reduces the latency and delay of data transmission. Thus, it is of importance to quantify the exact amount of latency reduction provided by the proposed CP-less OFDM scheme. Fig. 5.8 presents the transmission latency caused by regular OFDM with different CP lengths (which are equal to the delay spread of the channel) compared to that of the proposed scheme, where the alignment signal is used instead of CP, under the effect of different channel delay spreads. It is evident from the figure that the delay caused by regular OFDM increases as the CDS gets longer since the CP period extends more in time to protect against time dispersion, and thus the whole OFDM transmission time increases. On the other hand, CP-less OFDM scheme shows fixed transmission delay at all CDS values (i.e., it is delay spread-independent). This is due to the fact that the alignment signal does not occupy any temporal resources as it is just superimposed and added on top of the OFDM symbol in the power domain. Thus, the transmission latency of CP-less OFDM is always equal to the time period of useful data part of the CP-less OFDM symbol.

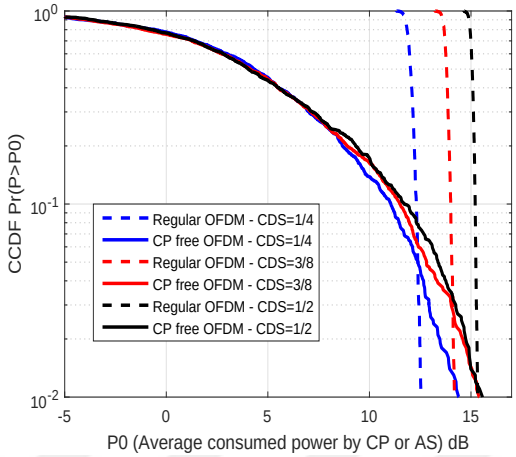


Figure 5.9: Power efficiency comparison between CP-less OFDM and CP OFDM for different channel delay spread length. Modulation is QPSK, N=64, and DF=1.

5.4.4 Power Efficiency

Since the proposed CP-free OFDM scheme totally eliminates the CP guard period, the power consumed by CP in regular OFDM will be saved. However, the proposed scheme on the other hand uses AS which also consumes a certain amount of power to suppress the ISI and provide circularity. Therefore, it is intuitively expected that there will be a trade-off relation between the power saved due to not using CP and the power consumed due to using AS. Accordingly, it would be interesting if we compare the power efficiency of CP-less OFDM with that of regular CP OFDM.

Fig. 5.9 plots the complementary cumulative distribution function (CCDF) of the sum power consumed by the CP part of regular OFDM, and the sum power distribution of AS (which is function of the channel) used in CP-less OFDM versus different CDS values when DF=1. The figure shows that the power consumed by AS increases slightly as the CDS increases, whereas the power consumed by CP increases significantly as CDS goes higher. As shown from the figure, the total average power consumed by AS is just 0.05 percent of the time greater than that consumed by CP when CDS=1/4 and it is about 0.01 percent of the time when CDS=1/2. In other words, the probability that the power consumed by AS

greater than that of the CP is 0.01 when CDS=1/2. Based on these results, one can conclude that the power efficiency of the proposed CP-less OFDM is much better that that of regular CP OFDM scheme. This specific merit makes the proposed design suitable for green type communication, which is very crucial requirement for future environmentally friendly and health-friendly communication systems.

5.4.5 Secrecy Performance

Besides the aforementioned verified and validated advantages of the proposed CP-less OFDM scheme in terms of low equalization complexity at the Rx, enhanced spectral efficiency, reduced latency, and better power efficiency; there is another extra advantage related to providing physical layer security against eavesdropping [95]. This additional merit related to security comes for free as a result of designing alignment signals dependent on the channel of the legitimate receiver, which is naturally different from that of the eavesdropper whose location is normally assumed distant by at least half wavelength from that of the legitimate receiver [52, 95]. Consequently, a secrecy gain will occur as the added AS (which is function of the legitimate receiver's channel) at the Tx will not be aligned or canceled at the eavesdropper side, but rather causing extra interference and resulting in a tangible degradation in the performance.

To investigate the secrecy performance provided by the proposed scheme, we use BER-based secrecy gap between the legitimate receiver and eavesdropper as a security performance measure [52, 71, 95]. Fig. 5.10 presents the secrecy performance of the proposed CP-less OFDM using BER secrecy gap versus SNR at different channel decaying factors (DF). It is clear from the figure that the eavesdropper performance is worse than that of the legitimate receiver. For instance, when DF=1, there is a gap of around 10 dB between the two receivers (i.e., the legitimate receiver and eavesdropper) at BER=10^{-2}. Such a large gap in performance can allow providing quality of service (QoS)-based security services [33], where the BER of the legitimate receiver is made less than a target BER (e.g.,

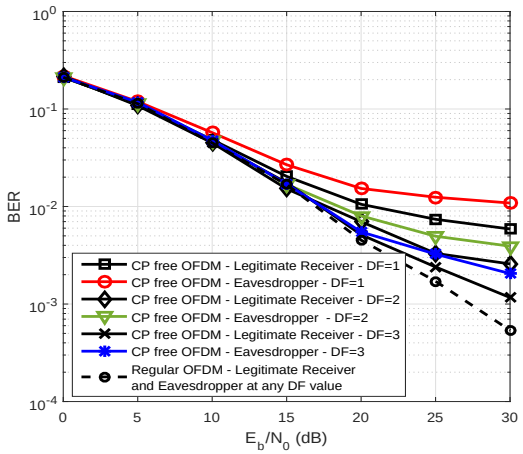


Figure 5.10: Secrecy performance of the proposed CP-less OFDM using BER secrecy gap between the legitimate receiver and eavesdropper versus SNR at different channel decaying factors (DF). Modulation is QPSK, N=64, and CDS=3/8.

BER=10^{-2}) to satisfy the required quality of a certain service (e.g., voice service), while eavesdropper's BER is made above this target BER to prevent eavesdropper from satisfying the QoS required for that specific service. It should be noted that this performance gap, which is obtained by considering uncoded system, may get smaller when advanced channel coding is used. Thus, it would be interesting to consider studying and investigating the effect of different coding schemes on the performance gap between Bob and Eve. This is left for future research studies on this topic as it is beyond the scope of this paper.

5.4.6 Robustness against Channel Estimation Errors

To evaluate the robustness of the proposed CP-less OFDM scheme against imperfect channel estimation, we add intentional errors denoted by ($\mathbf{\Delta h}$) to the true channel ($\mathbf{h}$) in order to obtain new erroneous channels given by $\hat{\mathbf{h}} = \mathbf{h} + \mathbf{\Delta h}$ [52]. $\mathbf{\Delta h}$ is modeled as an independent complex Gaussian noise with zero mean and variance $\sigma^{\mathbf{2}} = mse \times 10^{\frac{-SNR_{dB}}{10}}$, where mse is a variable related to the mean square error of the estimator's quality. Then, the alignment signal is designed based on this erroneously estimated channel $\hat{\mathbf{h}}$, which is different from the true channel $\mathbf{\Delta h}$. Fig. 5.11 presents the performance under different estimation qualities with

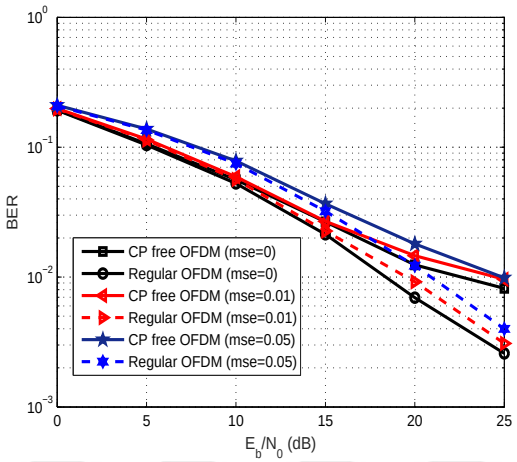


Figure 5.11: BER comparison between CP-less OFDM and CP OFDM with imperfect channel estimation factors when the channel delay spread (CDS) length is equal to one forth of the OFDM symbol period and decaying factor (DF) is 1. Modulation is 16-QAM and the number of subcarriers is N=64.

$mse = 0$ (perfect estimation), $mse = 0.01$ and $mse = 0.05$. It is shown that imperfect channel estimation leads to a small degradation due to having error mismatch between the alignment signal generated from the estimated channel and its actual value coming from the true channel. This results in a small performance degradation in the BER as the added alignment signal in this case will not perfectly cancel the actual interference coming from the true channel. However, this degradation can be further mitigated by increasing the length or power of the training sequence.

5.4.7 PAPR and OOBE

In order to check how AS affects the other critical waveform characteristics in terms of out-of-band emission (OOBE) and peak-to-average-power ratio (PAPR), we also plot the CCDF of PAPR and power spectral density (PSD) in Fig. 5.12 and Fig. 5.13, respectively. Due to the usage of an additional signal, a very small increase in PAPR and OOBE ($<$ 0.2 dB) is observed which is not considerably effective in system performance.

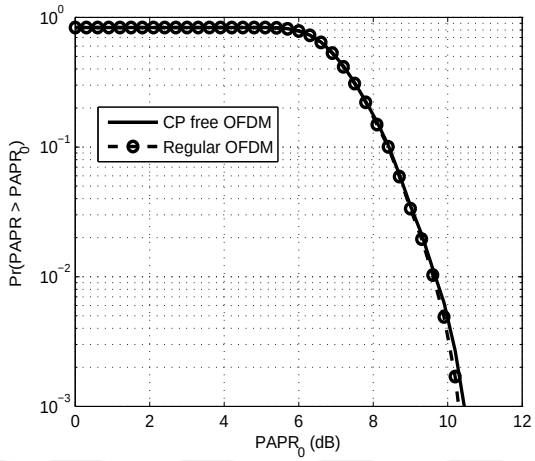


Figure 5.12: PAPR comparison between CP-less OFDM and CP OFDM. Modulation is 16QAM, N=64, CDS=1/8, and DF=2.

5.4.8 Complexity

It should be stated that the proposed CP-less OFDM scheme costs extra number of multiplications compared to conventional CP-OFDM. The extra processing cost at the transmitter is resulted from the need to calculate: 1) the aligning matrix $\mathbf{P}$ that consists of the null space vectors of $\mathbf{BH_u}$ with complexity of $O(N^2(N-R))$, and 2) the added signal $\mathbf{w}$, which is function of the inverse term given by $(\mathbf{HP})^{-1}$ with complexity of $O(N(N+R)R)$. However, due to the sparsity nature of the channel Toeplitz matrix $\mathbf{H}$ where there are many zero elements, the computational complexity of the proposed scheme can be significantly reduced by using advanced computing algorithms that take sparsity into account [115]. In particular, a sparse matrix can be solved with efficient algorithms that are capable of reducing complexity from $O(N^2)$ to $O(N)$, which represents linear complexity with sparse representation. Thus, the net complexity of the proposed scheme can at least be reduced to $O(\sqrt{(N-R)N^2}) + O(\sqrt{N(N+R)R})$.

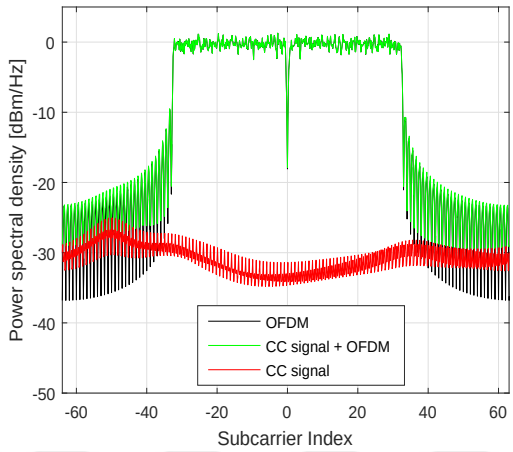


Figure 5.13: OOBE comparison between CP-less OFDM (with CP Canceling (CC) signal) and CP OFDM. Modulation is 16QAM, N=64, CDS=1/8, and DF=2.

5.4.9 Compatibility with MIMO

Since multiple-input multiple-output (MIMO) is an essential technology that has been adopted in 4G and 5G systems to enhance their performances in terms of data rates and reliability. The applicability of the proposed scheme for MIMO is highly desirable. It should be stated that although the structure of the proposed scheme is based on OFDM waveform, which is known for its easy integration with MIMO [2] due to its orthogonality where simple equalization can be performed for each subcarrier and antenna separately; CP-less OFDM scheme, which is proposed for SISO systems in this work, may require some modifications to make it fully compatible with MIMO due to having multiple channels interaction that may impact the orthogonality among subcarriers when CP is not used. Therefore, the compatibility of the proposed scheme with different modes of MIMO (such as transmit diversity, spatial multiplexing, and spatial modulation) will be subject of future research studies as this is beyond the scope of this paper.

5.5 Conclusion and Future Work

This work has proposed a CP-free OFDM design that eliminates the need of using excessive CPs between OFDM symbols. The design is shown to increase the spectral efficiency, enhance power efficiency, reduce latency, and improve physical layer security while maintaining low receiver complexity, making it a strong candidate for meeting the requirements of future 5G and beyond services and applications. Particularly, a novel power domain-based method that removes the requirement of CP while keeping the whole detection process the same at the receiver side is achieved by using a special design of alignment signals. These signals are added in the power domain of the transmitted OFDM symbols in order to achieve two goals simultaneously: 1) removing the inter-symbol-interference between symbols and 2) making the signal circular at the receiver side. Simulation results showed that spectral and power efficiency got enhanced, latency got reduced, and secrecy got improved while maintaining low complexity equalization at the Rx side.

Future work: Most of the performance aspects shown in Fig. 5.3 have been investigated in this paper. However, still there are other important aspects related to CP-less OFDM with AS which need to be studied and deeply investigated such as the effect of timing and carrier synchronization issues and how it should be performed in the proposed CP-free scheme. Moreover, channel estimation and how to handle error mismatch are also important issues to deal with. Besides, quantifying and checking the suitability of using the proposed scheme as a physical layer security technique for providing secrecy is as significant as the other performance measures. In addition, measurements and practical test bed implementations are also needed in order to validate the advantages of the proposed scheme and compare simulations with real conditions. All these factors and aspects are promising future research directions to be conducted in upcoming studies so that a complete picture of the proposed design including its merits and demerits can be carefully drawn and fully understood. As a final challenge, it is very substantial to come up with mathematical tools and techniques that can enable finding an accurate (or very close to accurate) inverse of the channel tall

overdetermined matrix that appears in the calculation of the AS signal. This will help guarantee having precise, accurate AS that ensures causing no interference and thus having intact BER performance.

Chapter 6

Secure, Adaptive Orthogonal Transform Division Multiplexing (OTDM) Waveform for 5G and Beyond

6.1 Introduction

Due to the inherent vulnerability of wireless systems to eavesdropping, designing practical physical layer security techniques is of extreme importance in order to provide confidential communication, especially for 5G and beyond systems [2]. The current encryption-based techniques are not sufficient considering the increasing computational power of future devices. Furthermore, the implementation, management, and distribution of keys are not easy tasks especially in de-centralized networks [6]. To address these problems, channel-based security approaches have emerged as a promising solution. Practical security based on signal processing methods can be provided by exploiting the spatial degree of freedom that exists in systems like MIMO, CoMP, relay, etc. However, there has recently been an interest in designing schemes that can provide security even

when there is no spatial degree of freedom. Among the ways to meet this is developing techniques tailored to common waveforms like OFDM or designing (from scratch) new inherently secure waveforms [116].

The physical layer security of OFDM was studied from an information-theoretic point of view in [117]. Based on the theoretical study, various OFDM security techniques have been proposed. These techniques can be classified from a high-level perspective into four main enabling approaches. First, adaptive transmission-based approaches, in which the transmission is adjusted to just meet the QoS requirements of the legitimate receiver. Among these approaches are optimal power allocation and pre-equalization [70], adaptive modulation and coding with adaptive automatic repeat request (ARQ) [33], and fading-based sub-carriers activation techniques [49]. Second, artificial noise (AN)-based schemes [50], in which the AN is designed based on the channel of the legitimate receiver and accumulated in the cyclic prefix at the receiver, resulting in an interference free reception of the OFDM symbol. Third, secret key-based schemes, where secret random sequences are extracted from the channel and then used to either encrypt the data bits on the application layer [68] or encrypt the data symbols on the physical layer such as constellation rotation and dynamic coordinate interleaving schemes [69]. Fourth, signal feature suppression techniques such as CP periodicity concealment [85].

As noticed, most of the aforementioned security techniques are tailored to OFDM-based systems. However, with the emersion of 5G and the possibility to use new waveforms (UFMC, GFDM, OTFS, etc.) that meet some specific requirements, it is also of significant importance to devise new waveforms that are inherently secure.

In this work, we propose a novel scheme that replaces the IFFT and FFT blocks, which are responsible for mapping symbols to sub-carriers in OFDM-based waveforms, by new blocks that can perform the modulation function in an inherently secure manner. Particularly, instead of using the fixed complex exponential transform bases (produced by IFFT and FFT) as information-bearing carriers, new orthogonal bases are extracted from the channel of the legitimate user and then used to carry and extract data at the transmitter and receiver

sides, respectively. The presented design not only provides security, but also enhances power efficiency, robustness against channel impairments, and reliability. Particularly, better BER performance is obtained for the legitimate user as a result of increasing the accumulated SNR. These merits could make the proposed waveform a strong candidate for future secure 5G and beyond systems.

The rest of the paper is organized as follows. The system preliminaries are described in Section 6.2. The details of the developed secure orthogonal transform division multiplexing (OTDM) waveform are revealed in Section 6.3. Section IV gives some insights on OTDM. Simulation results are discussed in Section 6.4, followed by a conclusion in Section 6.5.

Notations: Vectors are denoted by bold-small letters, whereas matrices are denoted by bold-large letters. $\mathbf{I}$ is the $N \times N$ identity matrix. The convolution operator is indicated by $(*)$. The transpose, hermitian (conjugate transpose) and inverse are symbolized by $(\cdot)^T$, $(\cdot)^H$ and $(\cdot)^{-1}$, respectively.

6.2 Preliminaries and Assumptions

A single-input single-output (SISO) system is considered. In particular, a transmitter (Tx), called Alice, needs to confidentially communicate with a legitimate receiver (Rx), called Bob, under the presence of an eavesdropper, called Eve. All received signals exhibit multi-path slowly varying Rayleigh fading channels. Also, the channel reciprocity property is adopted in our design, where the downlink channel (Alice to Bob) can be estimated from the uplink one (Bob to Alice), in a time division duplex (TDD) or hybrid systems (TDD with FDD). Moreover, since Eve is a passive node, the realistic assumption, where Alice has no knowledge of Eve's channel $\mathbf{H_e}$, is adopted. As a final notice, since the wireless channel is unique to the positions of the Tx and Rx, both Bob and Eve are assumed to experience independent channels.

6.3 Proposed Secure OTDM Waveform

The proposed secure waveform design is illustrated in Fig. 6.1. At the Tx, the total number of data symbols to be sent is N, where each transmission block is represented as $\mathbf{s} = \begin{bmatrix} s_0 & s_1 & ... & s_{N-1} \end{bmatrix}^T \in \mathbb{C}^{[N\times 1]}$. Each one of the complex baseband modulated symbols, s_i, is mapped to or carried by a channel-based orthogonal transform basis $\mathbf{v} \in \mathbb{C}^{[N\times 1]}$, where the mapping process is basically implemented via a simple multiplication operation between each data symbol and the orthogonal basis vector. For the N data symbols to be transmitted, we need N carrying orthogonal bases, which can be taken from the column vectors of $\mathbf{V}$, given by $\mathbf{V} = \begin{bmatrix} \mathbf{v}_0 & \mathbf{v}_1 & ... & \mathbf{v}_{N-1} \end{bmatrix} \in \mathbb{C}^{[N\times N]}$, where $\mathbf{V}$ is a transformation matrix, extracted from the legitimate user's channel. Also, each ith column vector (transform basis) in $\mathbf{V}$ can be expressed as $\mathbf{v_i} = \begin{bmatrix} v_0 & v_1 & ... & v_{N-1} \end{bmatrix}^T \in \mathbb{C}^{[N\times 1]}$.

Now, the key idea behind the proposed design is stemmed from the fact that the convolution process between a channel impulse response of L taps, $\mathbf{h} = [h_0, \cdots, h_{(L-1)}]$, and a transmitted data block $\mathbf{x}$ of length N can be represented by the linear multiplication of the Toeplitz matrix $\mathbf{H_b} \in \mathbb{C}^{[(N+L-1)\times N]}$ with $\mathbf{x}$. Since $\mathbf{H_b}$ represents a matrix, whose size is equal to the length of the transmitted data block added to the channel taps (i.e., $(N + L - 1)$) times the length of only the transmitted data block (i.e., N), Alice and Bob can extract channel-based sub-carriers (basis functions) by decomposing (performing orthogonal factorization on) $\mathbf{H_b}$.

This is made possible by applying any of the linear decomposition methods (SVD, GMD, UCD, etc.). For familiarity, SVD, a tool commonly used in MIMO systems [118]), is chosen as the underlying method. Thus, $\mathbf{H_b}$ can equivalently be expressed in-terms of three new matrices as follows:

$$\mathbf{H_b} = \underbrace{\mathbf{U}}_{\in\mathbb{C}^{[(N+L-1)\times N]}} \underbrace{\mathbf{E}}_{\in\mathbb{C}^{[N\times N]}} \underbrace{\mathbf{V}^H}_{\in\mathbb{C}^{[N\times N]}}, \tag{6.1}$$

where $\mathbf{U}$ and $\mathbf{V}^H$ are orthonormal matrices and $\mathbf{E}$ is a diagonal matrix with real entires. It should be noted that the number of orthogonal bases at the Tx depends on the columns' number of $\mathbf{V}$, which is equal to the transmitted data

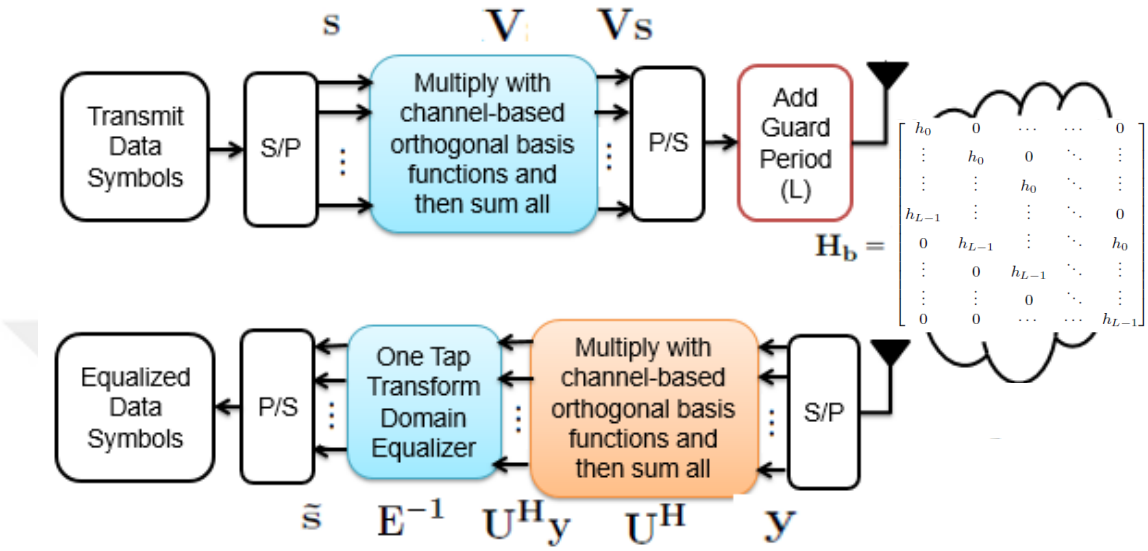


Figure 6.1: Structure of the designed baseband secure OTDM waveform.

block length (N). When the transmitted block gets convolved with the channel, then the number of orthogonal bases at the Rx depends on the columns' number of $\mathbf{U}^H$, which is equal to the number of data symbols plus the channel taps ($N + L - 1$). From (1), Alice can take the hermitian of $\mathbf{V}^H$ to get $\mathbf{V}$. Since the column vectors of $\mathbf{V}$ are orthogonal to each other, Alice can use them as basis functions (sub-carriers) to transmit symbols without interference. Alice maps each symbol to its corresponding basis function via simple multiplication, and then multiplex all the resulting multiplications as they are orthogonal to each other. This results in a block of samples, $\mathbf{x}$, referred to as one OTDM symbol. This process can mathematically be given as

$$\mathbf{x} = \sum_{i=0}^{N-1} s_i \mathbf{v}_i \in \mathbb{C}^{[N\times 1]}, \tag{6.2}$$

which can further be simplified into a matrix form as

$$\mathbf{x} = \mathbf{Vs} \in \mathbb{C}^{[N\times 1]}. \tag{6.3}$$

From a signal processing point of view, this is somehow similar to transmit pre-coding process in spatial multiplexing MIMO systems [118], but here it is in

the temporal domain of a SISO system. Furthermore, what looks like precoding is interestingly similar to the IFFT transform matrix in OFDM, and since $\mathbf{V}$ satisfies the transform properties, $\mathbf{V}$ can be seen as a transform matrix too, but extracted from the channel rather than being fixed as in OFDM.

Now, to avoid the interference between consecutive blocks, known as inter block interference (IBI), zero-padding (ZP), as a guard period interval with length equal to the channel delay spread L, is appended to the end of each block. This results in saving power resources compared to CP-OFDM, since no energy is sent in the ZP period. The baseband received OTDM symbol at Bob after S/P conversion can be given as

$$\mathbf{y} \;=\; \mathbf{h_b} * \mathbf{x} + \mathbf{z_b} \in \mathbb{C}^{[(N+L-1)\times 1]}, \tag{6.4}$$

where $\mathbf{y} = \begin{bmatrix} y_0 & y_1 & ... & y_{N+L-1} \end{bmatrix}^T$, in which $y_i = \sum_{l=0}^{L-1} h_l x_{(i-l)} + z_{b(i)}$, and $\mathbf{z_b} \in \mathbb{C}^{[(N+L-1)\times 1]}$ is the zero-mean complex additive white Gaussian noise (AWGN) at Bob. The convolution form can be written in a matrix form as

$$\mathbf{y} \;=\; \mathbf{H_b x} + \mathbf{z_b} = \mathbf{H_b V s} + \mathbf{z_b}. \tag{6.5}$$

At the receiver side, Bob applies SVD on the Toeplitz matrix of its available channel response, and then takes the hermitian of $\mathbf{U}$ to get $\mathbf{U}^H$. Since the column vectors of $\mathbf{U}^H = \begin{bmatrix} \mathbf{u}_0^* & \mathbf{u}_1^* & ... & \mathbf{u}_{L+N-1}^* \end{bmatrix}$ are orthogonal to each others, Bob can use them as inverse basis functions to optimally extract the data symbols from the received OTDM block without interference. This can be implemented as follows:

$$\hat{\hat{\mathbf{s}}} \;=\; \sum_{i=0}^{N+L-1} y_i \mathbf{u}_i^* \in \mathbb{C}^{[N\times 1]}. \tag{6.6}$$

After that, Bob uses $\mathbf{E} = diag \begin{bmatrix} e_0 & e_1 & ... & e_{N-1} \end{bmatrix}$ to perform simple one tap zero-forcing equalization process for $\hat{\hat{\mathbf{s}}}$ to get the final equalized data symbols block $\hat{\mathbf{s}}$. The reception processes (channel-based transformation and equalization) can further be simplified into a matrix form as

$$\hat{\mathbf{s}} \;=\; \mathbf{E^{-1}}\hat{\hat{\mathbf{s}}} = \mathbf{E^{-1}U^H y} = \mathbf{E^{-1}U^H}\left(\mathbf{H_b V s} + \mathbf{z}\right) \tag{6.7}$$

$$\;=\; \mathbf{E^{-1}U^H}(\mathbf{UEV^H V s} + \mathbf{z}) = \mathbf{s} + \mathbf{E}^{-1}\mathbf{U}^H\mathbf{z}. \tag{6.8}$$

The previous process clearly shows that the transformation performed on $\mathbf{y}$ using matrix $\mathbf{U^H}$, which consists of multiple orthogonal basis functions extracted from the channel, diagonalizes the channel response. This process is then followed by equalization, in the transform domain, using the diagonal matrix $\mathbf{E}$. Also, it is evident how the transformation matrix $\mathbf{V}$ used at the Tx cancels the effect of the right part $\mathbf{V}^H$ of the decomposed channel since their multiplication results in an identity matrix ($\mathbf{I}$). Similarly, $\mathbf{U^H}$ used at the Rx cancels the effect of the left part $\mathbf{U}$ of the decomposed channel. It should be noticed that the basis functions at Bob are longer than those at Alice due to channel spreading, allowing the receiver to optimally collect the spread energy in the guard period. However after the transformation process, the length of the received block becomes as that of the transmitter. This is different from OFDM, where the exponential basis functions of IFFT and FFT have the same length, resulting in a small energy loss since the spread part of the signal in the CP is usually discarded before FFT process. The exact gain due to this process will be shown in the simulation results section.

On the eavesdropper side, the captured signal is given by

$$\mathbf{y_e} \;=\; \mathbf{H_e x} + \mathbf{z_e} = \mathbf{H_e V s} + \mathbf{z_e}, \tag{6.9}$$

where $\mathbf{H_e} \in \mathbb{C}^{[(N+L-1)\times N]}$ and $\mathbf{z_e} \in \mathbb{C}^{[(N+L-1)\times 1]}$ are the complex Toeplitz channel response matrix and AWGN of Eve, respectively. Although Eve is assumed to have a complex receiver with full knowledge of the transmission technique, she will not be able to decode the data correctly. This is due to the fact that her channel is different from Bob's one, thus when she extracts orthogonal basis functions using SVD, she will have different basis functions from Bob, making her unable to decode. Also, even if Eve is considered to know the same basis functions as Bob, still she will not be able to decode because these functions are not optimized to her channel as the transformation at Alice is extracted from Bob's channel, but not Eve. In this miserable situation to Eve, she will be forced to perform an extremely exhaustive search process, trying to find some transformation matrices that might reduce errors. However, this would be impractical as the matrix size is relatively huge and the possible values are large. Also, since the time variation nature of wireless channels provides frequently updated randomness, the secure waveform design would be updated frequently, which further increases the security

robustness. Thus, from a signal processing perspective, it is almost impossible for Eve to decode the data correctly.

6.4 OTDM vs OFDM and Some Insights

Compared to OFDM-based systems, there are several important points, which should be emphasized. 1) IFFT processing at the Tx in OFDM is replaced by the pre-transformation matrix $\mathbf{V}$, in OTDM. 2) FFT processing at the Rx in OFDM is replaced by the post-transformation matrix $\mathbf{U^H}$. 3) The Frequency domain equalization in OFDM is substituted in OTDM by a transform domain equalization process, with the same complexity as that of OFDM. 4) The cyclic-prefix in CP-OFDM is replaced by a ZP guard period with the same length as the delay spread of the channel. This means that cyclic convolution in OFDM is not required in OTDM as there is no need to go to the frequency domain to make equalization. 5) The fixed rectangular pulses, with shifted frequencies, in OFDM are replaced by channel-based orthogonal bases, whose length at the Rx is greater than those at the Tx by channel spread length. This allows the Rx to collect the energy in the ZP period, instead of removing it as in OFDM. 6) OTDM has the power efficiency advantage of zero padding (ZP)-OFDM system, since a zero-suffix guard period of length equal to the channel spread is used instead of the CP. 7) Unlike OFDM, in which synchronization can be achieved by either exploiting the CP or by sending a training sequence, in OTDM, only training-based algorithms can be used because there is no CP in OTDM. 8) The channel estimation in OTDM is foreseen to be similar to OFDM as both of them are block-based transmission techniques. Thus, the delay spread and number of taps of the channel can be determined by performing time-based or frequency-based channel sounding techniques. 9) OTDM is specifically designed to work best over frequency selective channels, which is the case in most broadband systems. Therefore, the proposed design needs some modifications to make it applicable for flat fading channels (this can be a subject of future research). 10) Since OTDM updates its bases based on the channel, this requires extra processing than OFDM.

6.5 Simulation Results

Simulations are performed to investigate the performance of OTDM by choosing BER as a security metric [6] [116]. We consider an OTDM system with $N = 64$ modulated QPSK data symbols and a ZP of length $L = 9$, which is equal to the number of taps in the channel. For the sake of fair comparison, we also consider a standard OFDM system with $N = 64$ active sub-carriers and a CP of length L. In order to focus on the security design concept, we consider for both schemes (OTDM and OFDM) uncoded non-adaptive loaded systems with simple zero-forcing equalization. Thus, the effect of coding, complex equalization and adaptive loading with optimal power allocation is left as a future research. Fig. 6.2 shows the BER of a legitimate Rx, employing the proposed OTDM (channel-based transforms), compared to OFDM (Fourier-based transform). It is shown that at BER=10^{-3}, OTDM outperforms OFDM by at least 3 dB and 5 dB for the cases of exponentially decaying and uniformly distributed power delay profiles with $L = 9$, respectively. Uniform profile gives better BER than exponential due to the fact that the former has equally significant spreading gain over all taps, while the later has an insignificant gain at most of its high ordered taps (i.e., the last $(L-1)$th taps) due to the decaying nature of the channel. Thus, the accumulated energy from the ZP period in the case of uniform profile is higher than that of the exponential profile, resulting in a lower BER. Moreover, Fig. 6.2 shows that the performance depends on the number of taps. In specific, Bob's BER gets enhanced as the number of taps increases from $L = 9$ to $L = 12$ due to having more signal energy spread in the ZP when the channel length is longer. From another perspective, the way the interference leakage in the guard period is gathered in the presence of noise using $\mathbf{U}^H$ is optimal as less noise is accumulated with the signal energy. This results in a higher SNR, leading to a better BER. This is dissimilar to OFDM, in which the guard period, containing the dispersed signal energy, is discarded before the FTT process.

Additionally, Fig. 6.2 depicts the degraded BER performance of Eve even though she is assumed to be fully aware of the method and uses the same transform matrix as Bob. This happens due to the use of channel-dependent waveforms

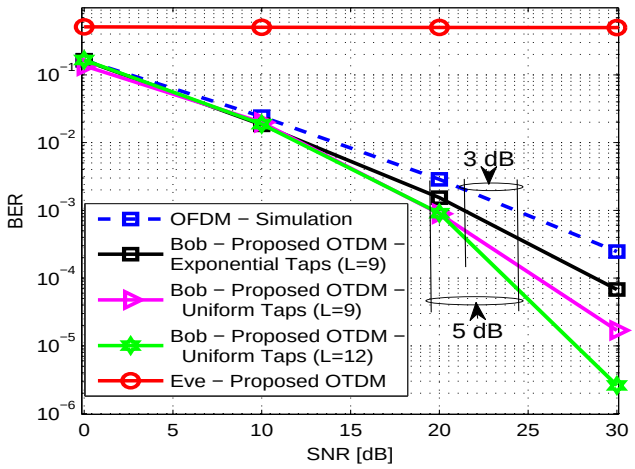


Figure 6.2: BER comparison between OFDM and OTDM with QPSK.

over Alice-to-Bob channel, which are different from Alice-to-Eve channel. As a result, the system response will not be diagonalized and a severe inter-symbol interference between data symbols will occur with respect to Eve.

To assess the robustness of our scheme against imperfect channel estimation (ICE), we add intentional errors at both the Tx and Rx ($\mathbf{\Delta h}_{T/R}$) to the true channel ($\mathbf{h}$) in order to obtain new erroneous channels given by $\hat{\mathbf{h}}_{T/R} = \mathbf{h} + \mathbf{\Delta h}_{T/R}$. $\mathbf{\Delta h}$ is modeled as an independent complex Gaussian noise with zero mean and variance $\boldsymbol{\sigma^2}_{T/R} = a \times 10^{\frac{-SNR_{dB}}{10}}$. Fig. 6.3 presents the performance under different estimation qualities with $a = 0$ (perfect estimation), $a = 0.01$ and $a = 0.1$. It is shown from Fig. 6.3 that ICE leads to a small degradation due to the error mismatch between the generated transforms $\hat{\mathbf{V}}$ and $\hat{\mathbf{U}}^H$ at the Tx and Rx sides, respectively, and their actual values coming from the true channel. This results in a small ISI between the data symbols as $\hat{\mathbf{V}}$ and $\hat{\mathbf{U}}^H$ extracted from the estimated channel will not perfectly cancel the effect of $\mathbf{V}$ and $\mathbf{U}^H$ coming from the true channel. However, this degradation can be overcome by increasing the length or power of the training sequence.

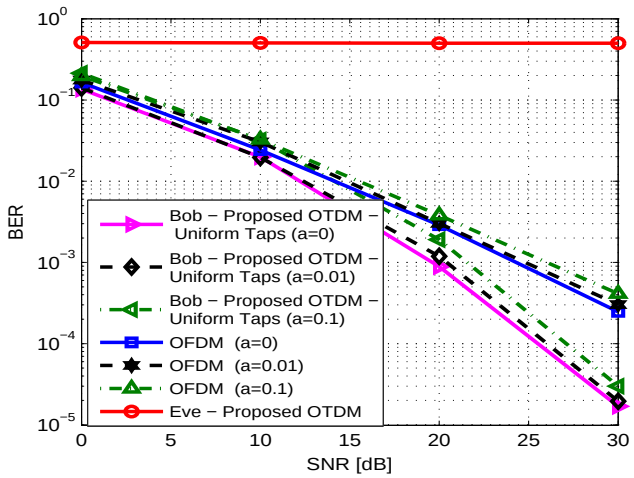


Figure 6.3: The effect of imperfect channel estimation on OTDM.

6.6 Conclusion

This work has proposed a 5G waveform design for providing physical security over dispersive channels. Particularly, orthogonal basis functions are extracted from the legitimate channel and then used as data bearing carriers instead of the exponential functions in OFDM. Thus, channel-based transformations are used instead of Fourier transforms to diagonalize the channel response of only the legitimate receiver. Besides security, the scheme is shown to enhance reliability, power efficiency and robustness against channel impairments.

Chapter 7

Time-Frequency Characteristics and PAPR Reduction of OTDM Waveform for 5G and Beyond

7.1 Introduction

OFDM has been the most dominantly used transmission scheme in the vast majority of the current broadband systems, such as LTE, WiFi and DVT. It has been adopted due to its desirable features, including higher spectral efficiency, simple equalization in the frequency domain, easy integration with MIMO systems and multi-user diversity, with the ability to flexibly schedule both time and frequency resources among users [90]. Nonetheless, OFDM has several major drawbacks, such as high peak-to-average power ratio (PAPR), spectral leakage, strict synchronization requirement and frequency offset sensitivity. Moreover, OFDM is proven to be a non-optimal transceiver design in terms of overall performance, and also lacks physical layer security features [52], which are very desirable in future 5G and beyond systems, making it inherently vulnerable to eavesdropping. Due to the aforementioned shortcomings, there has been a global consensus on the incapability of OFDM alone in satisfying all the needs of future networks and

their diverse expected applications, such as Tactile Internet, Machine to Machine (M2M) and Internet of Thing (IoT) [66]. Thus, researchers around the world have been trying to design new waveforms or different numerologies of OFDM to meet the requirements of future emerging 5G-enabled applications and scenarios [66].

In the literature [119] [120], many waveforms have been proposed to address some of the OFDM drawbacks. Among these are filtered-OFDM, windowed-OFDM, FBMC, UW-OFDM, GFDM, UFMC, ZT-DFT-s-OFDM, UW-DFT-s-OFDM, etc.

As inferred from the literature, most of the recently proposed waveforms for 5G systems are Fourier transform-dependent and designed without taking channel realizations into account. This kind of design comes with two major demerits. Firstly, it results in a non-optimal transceiver design, where the transmit and receive basis functions (pulses) are static and do not adapt to the channel variations. Secondly, it is vulnerable to wireless eavesdropping, where physical layer security has not been considered as a requirement in the aforementioned waveform designs. To address these problems, the authors in [52] proposed an adaptive channel-based transform waveform, called orthogonal transform division multiplexing (OTDM), for future secure 5G and beyond systems. In particular, instead of using fixed exponential basis functions, produced by IFFT and FFT as in OFDM, new orthogonal basis functions are extracted from the channel and used to securely modulate and demodulate the data symbols at the transmitter and receiver sides, respectively. This design results in two major merits over the currently existing waveforms in the literature. First, it provides physical layer security, a new important feature, which comes for free as a result of the channel-based design. Second, it enhances reliability and robustness against channel impairments, where better BER performance is obtained as a result of increasing the effective signal-to-noise ratio (SNR). The waveform design reported in [52] was presented from a pure security perspective, where the mathematical framework of the design was introduced and its immunity against eavesdropping was proven. However, the time-frequency characteristics of the basis functions of OTDM as well as its PAPR and their differences from OFDM were not investigated. Therefore, this paper comes to complement and build on top of the work presented in [52] to address the aforementioned issues. Specifically, we make the

following main contributions:

- We investigate and visualize the time and frequency characteristics of the basis functions of OTDM waveform, and show how their shapes vary for different channel realizations. Then, we exhibit their differences from the complex exponential basis functions of OFDM-based waveforms. This is performed in order to provide insights and an in depth understanding of the concept of channel-based transform waveforms.
- We examine the PAPR of OTDM and demonstrate how its distribution is the same as that of OFDM. Thus, this motivates finding an efficient PAPR reduction technique, specifically designed for OTDM waveform.
- By exploiting the fact that the deep-faded subchannels of the effective channel transform response in OTDM waveform are always localized and situated at the left edge of the OTDM block, we propose an effective method that exploits this feature for reducing its PAPR.

The rest of this chapter is organized as follows. The system model is described in Section 7.2. The OTDM waveform characteristics and their differences from OFDM are exhibited in Section 7.3. The details of the proposed PAPR reduction technique for OTDM are revealed in Section IV. Simulation results are discussed in Section 7.4. Finally, a concise conclusion is drawn in Section 7.5.[1]

7.2 Preliminaries and System Model

A single-input single-output (SISO) system, in which a transmitter (Tx), called Alice, is communicating with a legitimate receiver (Rx), called Bob, whereas an eavesdropper, called Eve, is trying to intercept the communication between the

[1] Notations: In this paper, vectors are denoted by bold-small letters, whereas matrices are denoted by bold-capital letters. $\mathbf{I}$ is the $N \times N$ identity matrix. Norm-2 and norm-infinity are defined by $\| \cdot \|_2$ and $\| \cdot \|_\infty$, respectively. The convolution, inverse, transpose and conjugate transpose operators are symbolized by $(\circledast)$, $(\cdot)^{-1}$, $(\cdot)^{\mathrm{T}}$ and $(\cdot)^{\mathrm{H}}$, respectively.

two legitimate parties (Alice and Bob). All received signals experience independent multi-path slowly varying Rayleigh fading channels [52]. Also, the channel reciprocity property is adopted, where the downlink channel can be estimated from the uplink one, in a time division duplex (TDD) system [56].

In the OTDM waveform design [52], channel-based transform basis functions are used as subcarriers for the complex baseband modulated symbols, s_i. The total number of data symbols in one transmission block $\mathbf{s} = \begin{bmatrix} s_0 & s_1 & ... & s_{N-1} \end{bmatrix}^{\mathrm{T}}$ is N. Each of s_i is carried by a specific channel-based orthogonal pulse $\mathbf{v} \in \mathbb{C}^{[N\times 1]}$, where the mapping process in this case is basically implemented via a simple multiplication operation between each data symbol and an orthogonal basis function. For the N data symbols to be transmitted, we need N carrying orthogonal basis functions, which can be taken from the column vectors of $\mathbf{V}$, given by

$$\mathbf{V} \;=\; \begin{bmatrix} \mathbf{v}_0 & \mathbf{v}_1 & ... & \mathbf{v}_{N-1} \end{bmatrix} \in \mathbb{C}^{[N\times N]}. \tag{7.1}$$

Hence, $\mathbf{V}$ can be seen as the channel-based transform matrix, which can be obtained by decomposing the channel matrix $\mathbf{H_b} \in \mathbb{C}^{[(N+L-1)\times N]}$ of the legitimate user's channel impulse response $\mathbf{h_b} = \begin{bmatrix} h_0 & h_1 & ... & h_{L-1} \end{bmatrix}^{\mathrm{T}}$ using SVD as follows

$$\mathbf{H_b} = \mathbf{UEV}^{\mathrm{H}}. \tag{7.2}$$

Note that $\mathbf{H_b}$ is an $(N + L - 1) \times N$ Toeplitz matrix with first column $\begin{bmatrix} h_0 & h_1 & \cdots & h_{L-1} & 0 & \cdots & 0 \end{bmatrix}^{\mathrm{T}}$ and first row $\begin{bmatrix} h_0 & 0 & \cdots & 0 \end{bmatrix}^{\mathrm{T}}$. Each ith column (basis function) in $\mathbf{V}$ can be expressed as $\mathbf{v_i} = \begin{bmatrix} v_0 & v_1 & ... & v_{N-1} \end{bmatrix}^{\mathrm{T}}$. After multiplying each symbol with its corresponding basis function, we multiplex and sum all the resulting vectors to get a block of samples, $\mathbf{x}$, referred to as one OTDM symbol. This process can mathematically be stated as

$$\mathbf{x} \;=\; \sum_{i=0}^{N-1} s_i \mathbf{v}_i, \in \mathbb{C}^{[N\times 1]}, \tag{7.3}$$

which can further be simplified into a matrix form as

$$\mathbf{x} \;=\; \mathbf{Vs} \in \mathbb{C}^{[N\times 1]}. \tag{7.4}$$

From a signal processing point of view, this looks similar to transmit pre-coding in spatial multiplexing MIMO, but here the matrix is extracted from the temporal (not spatial) variation of the channel. To avoid the inter-block interference (IBI), zero-padding (ZP) as a guard interval of length $L-1$, is appended to the end of each block. After OTDM block, $\mathbf{x}$, is sent through the channel, the received signal at Bob can be given as

$$\mathbf{y} = \mathbf{h_b} \circledast \mathbf{x} + \mathbf{z_b}, \tag{7.5}$$

$$y_i = \sum_{l=0}^{L-1} h_l x_{(i-l)} + z_{b(i)}, \tag{7.6}$$

where $\mathbf{y} = \begin{bmatrix} y_0 & y_1 & ... & y_{N+L-1} \end{bmatrix}^{\mathrm{T}}$ is the received block of one OTDM symbol and $\mathbf{z_b} \in \mathbb{C}^{[(N+L-1)\times 1]}$ is the zero-mean complex additive white Gaussian noise (AWGN) at Bob.

The previous convolution form can also be equivalently written in a linear algebraic matrix form as

$$\mathbf{y} = \mathbf{H_b x} + \mathbf{z_b} = \mathbf{H_b V s} + \mathbf{z_b} = \mathbf{UEs} + \mathbf{z}. \tag{7.7}$$

To remove the effect of the time dispersion caused by the channel spread at the Rx, a channel-based transformation process is performed on $\mathbf{y}$ using matrix $\mathbf{U}^H = \begin{bmatrix} \mathbf{u}_1^* & \mathbf{u}_2^* & \cdots & \mathbf{u}_{N+L-1}^* \end{bmatrix} \in \mathbb{C}^{[N\times(N+L-1)]}$. Each ith column (basis function) in $\mathbf{U}^{\mathrm{H}}$ can be expressed as $\mathbf{u}_i^* = \begin{bmatrix} u_0 & u_1 & ... & u_{N-1} \end{bmatrix}^{\mathrm{T}}$. The matrix $\mathbf{U}^{\mathrm{H}}$ consists of multiple orthogonal basis functions, which are optimally extracted from the channel and can be used as inverse basis functions to extract the transmitted block by diagonalizing the channel response. To do so, the Rx transforms $\mathbf{y}$ using $\mathbf{U}^{\mathrm{H}}$ as follows:

$$\sum_{i=0}^{N+L-1} y_i \mathbf{u}_i^* = \mathbf{U}^{\mathrm{H}}\mathbf{y} = \mathbf{Es} + \mathbf{U}^{\mathrm{H}}\mathbf{z} = \mathbf{Es} + \hat{\mathbf{z}}, \tag{7.8}$$

where $\hat{\mathbf{z}} = \mathbf{U}^{\mathrm{H}}\mathbf{z} \in \mathbb{C}^{[N\times 1]}$. It should be noted that the vectors of $\mathbf{U}^{\mathrm{H}}$ span not only the whole transmitted block time but also the following time reserved for ZP. After multiplying by $\mathbf{U}^{\mathrm{H}}$, the leakage energy of the signal due to channel spreading will be collected from the ZP optimally with minimal noise thanks to the optimal

extracted basis functions, whose length at the Rx is equal to the received OTDM signal's length. The estimated data symbols can be obtained by equalizing the effect of the diagonal matrix $\mathbf{E} \in \mathbb{C}^{[N \times N]}$, which contains the channel gain over each data symbol. Thus, the final equalized block of data symbols $\tilde{\mathbf{s}}$ can be obtained by performing simple one tap equalization in the transform domain as given below

$$\tilde{\mathbf{s}} = \mathbf{E}^{-1}\mathbf{U}^{\mathrm{H}}\mathbf{y} = \mathbf{E}^{-1}\left(\mathbf{E}\mathbf{s} + \mathbf{U}^{\mathrm{H}}\mathbf{z}\right) \tag{7.9}$$

$$= \mathbf{s} + \mathbf{E}^{-1}\mathbf{U}^{\mathrm{H}}\mathbf{z} = \mathbf{s} + \mathbf{E}^{-1}\hat{\mathbf{z}}. \tag{7.10}$$

7.3 Waveform Characteristics: OTDM vs OFDM

In most of the previously developed multi-carrier transmission methods, the orthogonal sub-carriers (basis functions), which are generated by IFFT and FFT at the Tx and Rx sides, respectively, are fixed and channel-independent. This design results in a static, channel-unaware, non-optimal, and insecure transmission. However, in the channel-based transform design, the orthogonal basis functions, on which the symbols are carried on, are directly extracted from the small scale multi-path channel and used at both the Tx and Rx to optimally diagonalize the channel. Here, we provide an in-depth investigation and comparison of the waveform shapes and time-frequency characteristics between channel-based transform and Fourier-based transform waveforms. Particularly, we pick OTDM as a waveform that represents channel-based transform waveform class and OFDM as another waveform that represents Fourier-based transform waveform class. Fig. 7.1 shows the major differences between the shape of the pulses in time and frequency domains of OFDM and OTDM waveforms. It is observed that for a certain channel response the time domain shapes of the basis functions in OTDM are multiple of half cosine pulses compared to fixed rectangular pulses in OFDM. Consequently, the frequency domain shapes of the basis functions in OTDM are different from OTDM as visualized in Fig. 7.1. On the other hand, Fig. 7.2 describes how the time and spectral shapes of the pulses change for different

channel realizations. This explains the adaptivity and security nature of OTDM and how it adopts to changing channels. Fig. 7.3 presents the effective channel transform response of OTDM obtained by $\mathbf{E}$ (on the left part of the figure), and its difference from the channel frequency response of OFDM (on the right part of the figure). As depicted, the subchannel gains in OTDM waveform are sorted in a descending order, and thus the deep-faded subchannels are localized at the edge of the effective channel transform response. This special feature will be exploited to design a channel-dependent PAPR reduction technique, as it will be explained in the next Section. On the contrary, the subchannel gains in OFDM waveform are not-sorted and the deep-faded subchannels are distributed over the whole channel frequency response.

7.4 OTDM with Edge Subcarrier Dedication (OTDM-ESD): PAPR Reduction Technique

Many techniques have been proposed in the literature to reduce the PAPR of OFDM waveform [121]. However, the direct implementation of these techniques on OTDM waveform will not be efficient and optimal in terms of the overall system performance. This is due to the fact that the OTDM characteristics are different from those of OFDM. Thus, by taking advantage of the inherent nature of OTDM, a more effective PAPR reduction technique can be devised. Here, we propose an efficient channel-dependent tone reservation (TR) technique to specifically reduce the PAPR of OTDM waveforms. The key idea is to exploit the inherent characteristics of the channel transform response of OTDM (shown in Fig. 7.3) in order to design a technique that not only reduces the PAPR, but also enhances the reliability performance, which is different from the conventional TR technique [121], in which the reserved subcarriers are not channel dependent. Particularly, the fact that deep-faded subchannels in OTDM are always localized at the edge of the effective channel response enables us to simply determine the number of subcarriers that are required to be used for PAPR reduction, and then assign the contiguous edge sub-carriers corresponding to the deep-faded

subchannels for PAPR reduction. Without loss of generality, in this method, we partition the OTDM block into two parts, in which the first part, which corresponds to good subchannels, is dedicated and used for data tranmission; while the second part, which corresponds to the deep-faded (bad) subchannels located at the edge of each OTDM block, is dedicated for PAPR reduction. By doing so, we ensure minimum capacity reduction as those subcarriers used for PAPR are already not good to be used for data transmission. Unlike the classical TR technique, a prior knowledge on the positions of the subcarriers used for PAPR reduction is not needed. In the proposed design, the transmitted signal can be modeled as

$$\mathbf{d} = \mathbf{GV}[\mathbf{s}\ \mathbf{w}]^{\mathrm{T}} \in \mathbb{C}^{[(N+L-1)\times 1]}, \tag{7.11}$$

where $\mathbf{s} \in \mathbb{C}^{[1\times(N-R)]}$ is a set of QAM symbols contained in a vector, $\mathbf{w} \in \mathbb{C}^{[1\times R]}$ is a set of samples to be optimized to reduce PAPR, $\mathbf{V}$ is the N-point channel-based transformation matrix, and $\mathbf{G} \in \mathbb{C}^{[(N+L-1)\times N]}$ is the ZP addition matrix. The PAPR of the above-transmitted signal is the ratio of the maximum transmitted power to the average power, which can be given as

$$PAPR = \frac{\|\mathbf{GV}([\mathbf{s}\ \mathbf{w}]^{\mathrm{T}})\|_{\infty}^{2}}{\frac{1}{N+L-1}\|\mathbf{GV}([\mathbf{s}\ \mathbf{w}]^{\mathrm{T}})\|_{2}^{2}}. \tag{7.12}$$

The problem here reduces to finding the optimal AN vector $\mathbf{w}$ that can effectively reduce the PAPR of the signal $\mathbf{d}$. Thus, the optimization problem to be solved can be formulated as

$$\begin{aligned} \mathbf{w}_{opt} &= \arg\ \min_{\mathbf{w}} \|\mathbf{GV}([\mathbf{s}\ \mathbf{w}]^{\mathrm{T}})\|_{\infty}^{2} \\ subject\ to &\rightarrow \|\mathbf{w}\|_{2}^{2} \leq \lambda \times \|\mathbf{s}\|_{2}^{2}, \end{aligned} \tag{7.13}$$

where the percentage of power used by $\mathbf{w}$ signal is controlled by λ. The objective function shows that we have a convex optimization problem that can numerically be solved by some advanced and powerful convex optimization solvers such as MOSEK. In this case, to obtain a precise numerical solution to the optimization problem in our hands, we adopt using YALMIP, a handy optimization package that can be integrated with MOSEK and MATLAB to solve complex problems.

7.5 Simulation Results

In this section, we provide simulation results to demonstrate the effectiveness of the proposed OTDM-ESD technique in reducing the PAPR and enhancing the BER performance as well as its performance comparison with OTDM and OFDM waveforms. We consider an OTDM system with $N = 64$ modulated QPSK data symbols and a guard period of length L. The channel is modeled as an independent and identically distributed (i.i.d.) block-fading, where channel coefficients are drawn according to an i.i.d. Rayleigh fading distribution at the beginning of each block transmission, and remain constant within one block, but change independently from one to another. The Rayleigh multi-path fading channel has nine taps $L = 9$ with an exponential power delay profile. Additionally, we assume an eavesdropper, who uses its channel to extract its basis functions, trying to intercept the communication. For the sake of fair comparison, we also consider a standard OFDM system with $N = 64$ active sub-carriers and a cyclic prefix (CP) of length L. Fig. 7.4 shows the bit error rate (BER) performance gain of a legitimate Rx, employing OTDM waveform compared to OFDM using the same parameters. It is shown that OTDM outperforms OFDM by at least 3 dB at BER=10^{-3} and that the gain increases as the SNR increases. This gain is obtained as a result of not discarding the leaked energy, but instead collecting it optimally by adopting the shape and length of the receive orthogonal basis functions according to the channel spread, in such a way that the total response of the system is diagonalized. Fig. 7.4 also presents the BER enhancement delivered by the OTDM-ESD technique for PAPR reduction. It is shown that there is around 4 dB gain compared to OTDM, and around 7 dB gain compared to OFDM. The resulting gain is due to dedicating the right edge sub-carriers corresponding to the deep-faded subchannels for PAPR reduction, instead of using them for data transmission. In other words, the gain is obtained as a result of avoiding the usage of the low subchannel gains that are responsible for limiting the system performance; instead, they are used for PAPR reduction and then discarded at the Rx.

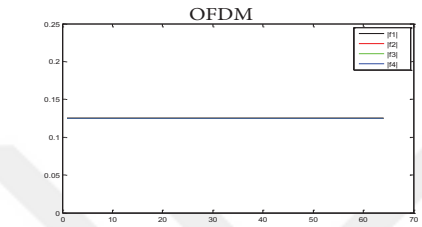
Moreover, it is shown that the gain of a uniformly distributed power delay profile is more than that of a channel with exponentially distributed power delay

profile. This is because uniform profile has equally significant spreading gain over all taps, while exponential profile has an insignificant gain at most of its high ordered taps due to its fast decaying nature. Thus, the accumulated energy from the ZP period in the case of uniform profile is higher than that of the exponential profile, resulting in a much lower BER. Additionally, Fig. 7.4 depicts the very bad BER performance of Eve although she is assumed to be fully aware of the method. This happens due to the use of channel-dependent waveforms through Alice-to-Bob channel, which are different from Alice-to-Eve channel. Thus, the system response will not be diagonalized for Eve. This will results in a severe inter-symbol interference between data symbols with respect to Eve.

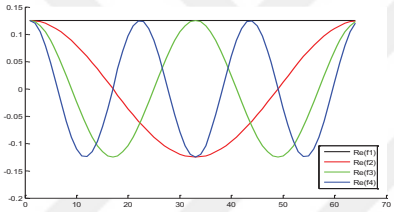
Fig. 7.5 explicitly shows that the PAPR of OTDM is the same as that of OFDM because both waveforms represent multi-carrier block based transmission schemes. However, when the proposed OTDM-ESD technique is applied by reserving only 8 subcarriers as peak reduction tones, significant PAPR reduction gain is achieved. Also, it is observed that the PAPR reduction gets better as the power of the peak reduction tones increases. These results prove the benefits of OTDM-ESD.

7.6 Conclusion

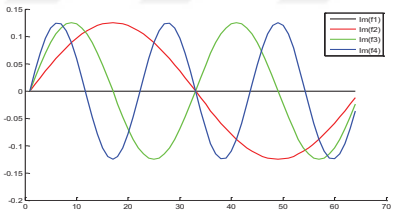
In this paper, we have investigated the characteristics of a new candidate 5G waveform, called OTDM. For this purpose, we have provided thorough comparison between OTDM and OFDM. Particularly, we presented the time and frequency domain shapes of its basis functions (pulses), which are extracted from the wireless channel, and showed how they change for different channel realizations. Moreover, we have examined the PAPR performance of OTDM compared to OFDM, and then presented an effective technique for reducing it.



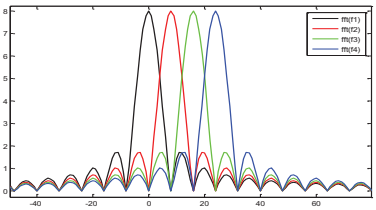
1: Time domain signals of the first four basis functions of F.



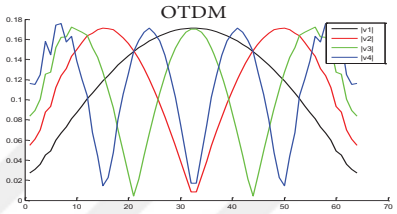
2: Real part of the time domain signals.



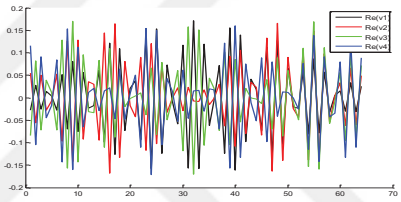
3: Imaginary part of the time domain signals.



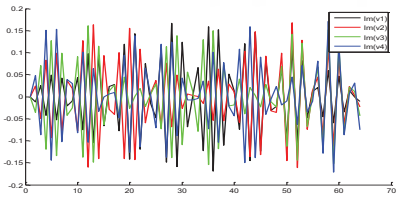
4: Frequency domain signals of the first four basis functions of the inverse fast Fourier transform matrix (i.e., subcarriers).



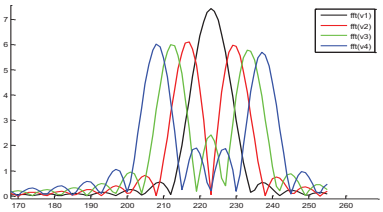
5: Time domain signals of the first four basis functions of V.



6: Real part of the time domain signal.



7: Imaginary part of the time domain signals.



8: Frequency domain signals of the first four basis functions of V transform matrix (i.e., subcarriers).

Figure 7.1: Waveform comparison between OFDM and OTDM in terms of the: 1) amplitude, 2) real part, 3) imaginary part, and 4) frequency shapes of the first four basis functions of the inverse Fourier and channel-based transform matrices given by $\mathbf{F}^{\mathrm{H}}$ and $\mathbf{V}$ (extracted from a channel with $L = 9$ taps), respectively.

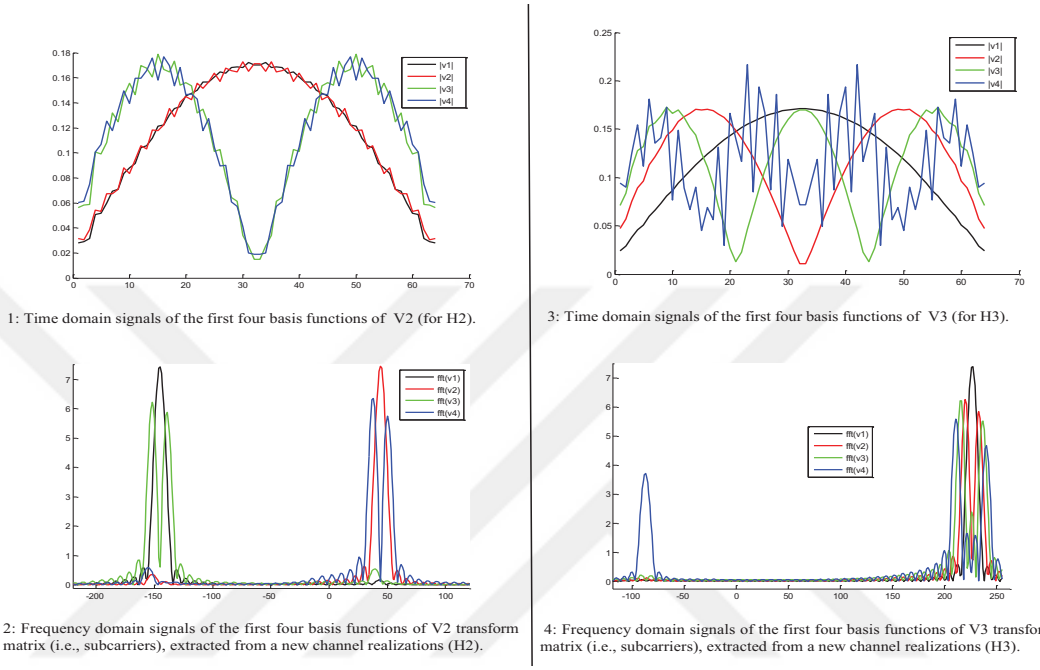


Figure 7.2: Time-frequency characteristics of the first four basis functions for two different channel realizations with $L = 9$ exponentially decaying taps.

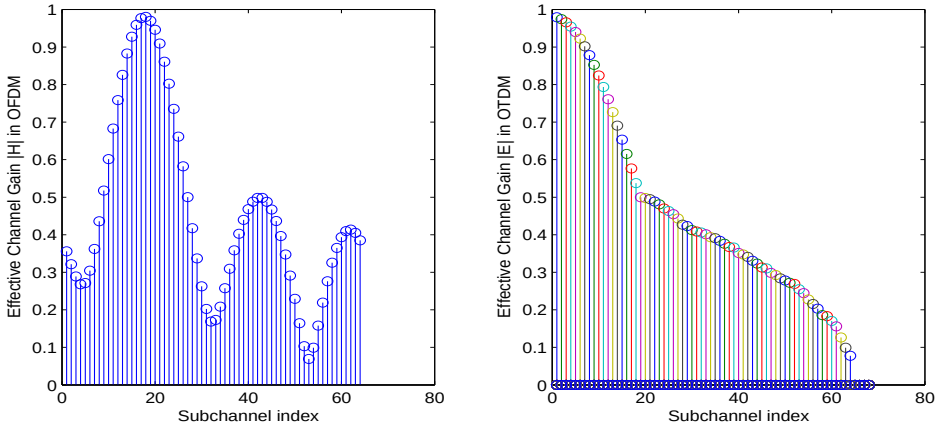


Figure 7.3: Comparison between the effective channel transform responses of OFDM (left shape) and OTDM (right shape).

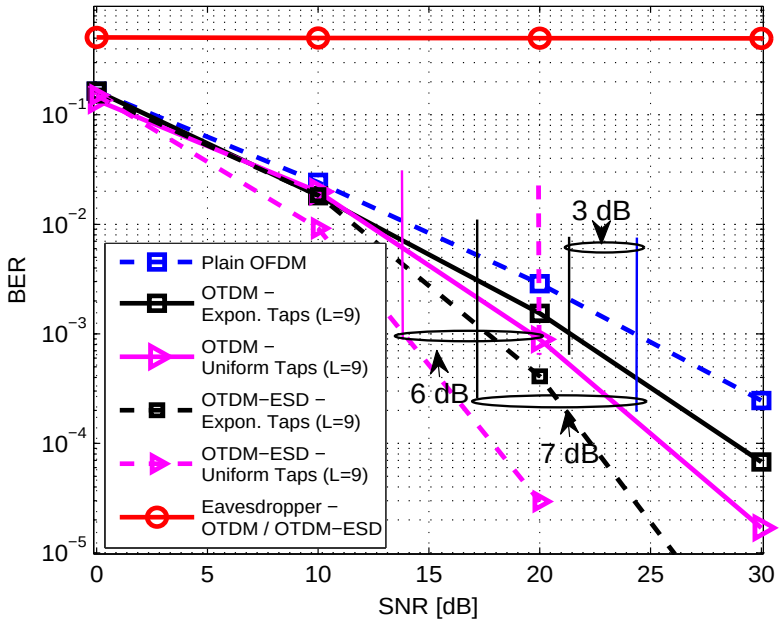


Figure 7.4: BER comparison of OTDM-ESD with OTDM and OFDM.

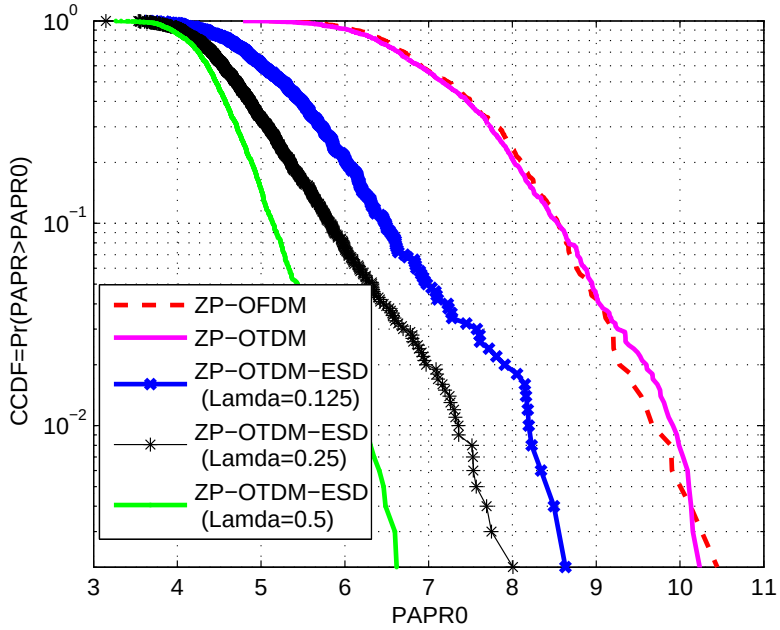


Figure 7.5: PAPR comparison of OTDM-ESD with OTDM and OFDM.

Chapter 8

A Practical Physical-Layer Security Method for Precoded OSTBC-Based MISO Systems

8.1 Introduction

The secrecy capacity of MIMO based communication systems have been studied for various scenarios from an information theoretic point of view [122–124]. Artificial noise along side optimal power allocation in MIMO systems are also investigated for security as in [48]. Additionally, beam-forming MIMO based security procedures have been examined in [125]. The effect of imperfect channel estimation on the secrecy capacity of MIMO systems has also been analyzed in [23, 126]. Methods based on beam-forming with optimal power allocation using artificial noise mechanism in MISO scenarios have been studied in [127], and for the SVD-based precoding scheme in [128]. For more details on MIMO based security methods and schemes, see [6, 22, 129].

In [130], a received signal strength (RSSI) based technique was suggested to protect the confidentiality of orthogonal space-time block-coding (STBC) using a shared, secret key generated from RSSI. In [131], another shared key based

encryption method is proposed for securing STBC, in which the transmitter randomly changes and alters the form of symbols based on precryptocoding matrix to prevent the attacker from getting the correct transmitted symbol. On the contrary to [130, 131], authors of [132] proposed a secure STBC without using a shared key. They used a full rate STBC scheme that permits independent decoding at the legitimate receiver but not at the malicious eavesdropper. They also increased the secrecy by adding aligned artificial noise. In [64], authors used precoding matrix indicator (PMI) in MIMO (spatial multiplexing mode) as a secret key assuming that PMI is only known by the legitimate parties.This is achieved by using channel sounding method and preventing the need for sending any feedback messages about PMI through the air.

However, in practical wireless systems (FDD/TDD), the selected PMI at the receiver side is usually fed back to the base station (eNodeB) via publicly accessed channel to avoid the problem of PMI mismatch selection due to imperfect channel reciprocity. This enables Eve to access the PMI and then make use of it. Additionally, in case there is no explicit feedback, still Eve can know the selected PMI by doing exhaustive search process in the available codebook and find out the used PMI. Motivated by these practical issues, this paper comes to address the problem of Eve's ability in knowing the selected PMI, which results in a small security performance.

To the best of our knowledge, we show for the first time in the literature from a practical perspective that the use of PMI alone in POSTBC MISO system can provide a small security gap region, considering the worst security scenario, where Eve is fully aware of the selected PMI. Then, we solve the problem of having small security gap through providing a practical power efficient security technique based on precoded OSTBC along-with partial pre-equalizing (PCPPE). In our proposed method, physical security is attained without using artificial noise as it causes waste in power resources, nor using secret key sharing as it might be cracked. Therefore, the developed green scheme can be integrated with current wireless systems such as LTE.

The rest of this chapter is organized as follows: system model is described in Section 8.2, followed by the security performance investigation of POSTBC in

Section 8.3. The details of PCPPE method are presented in Section 8.4. Then, simulation results are discussed in Section 8.5. Finally, a conclusive summary is drawn in Section 8.6.

8.2 System Model and Preliminaries

As depicted in Fig. 8.1, a multiple input single output (MISO) communication system employing precoded OSTBC is adopted. The complex baseband modulated symbols are gathered into groups, where each contains two symbols arranged using Alamouti STBC block. Accordingly, each two successive symbols x_1 and x_2 are encoded with the space-time codeword matrix given as

$$\mathbf{X} = \begin{bmatrix} x_1(n) & -x_2^*(n) \\ x_2(n) & x_1^*(n) \end{bmatrix}.$$

Hence, $\mathbf{X} \in C^{M \times T}$ is considered as the space time codeword of length M symbols with T period, where $*$ is the complex conjugate operator. In MISO system with N_T transmit antennas, POSTBC is usually applied to exploit the full diversity of the channel by achieving orthogonal transmission among the parallel channels such that interference between the transmitted signals is reduced. This is implemented through multiplying the space time code $\mathbf{X}$ by a precoding matrix $\mathbf{W}$ chosen from a universal codebook composed of a set of precoding matrices, that are stored at both the transmitter and receiver sides.

In particular, a trusted sender, Alice, conveys data packets to a legitimate receiver, Bob. Each packet consists of multiple consecutive precoded space-time codewords ($\mathbf{WX}$). The baseband received signal at the side of Bob in the first and second time slot is given in (1) in matrix form and in (3) in expanded form, where $\mathbf{H^b} \in C^{1 \times N_T}$ is the complex gain vector of N_T transmit antennas. Each antenna (independent of the others) experiences a one-tap channel with constant gain over one packet length, but i.i.d. from one packet to another. $\mathbf{z^b}$ is the zero-mean complex additive white Gaussian noise (AWGN). An eavesdropper, Eve, tries to receive the signal transmitted by Alice. Similarly, the signal captured by

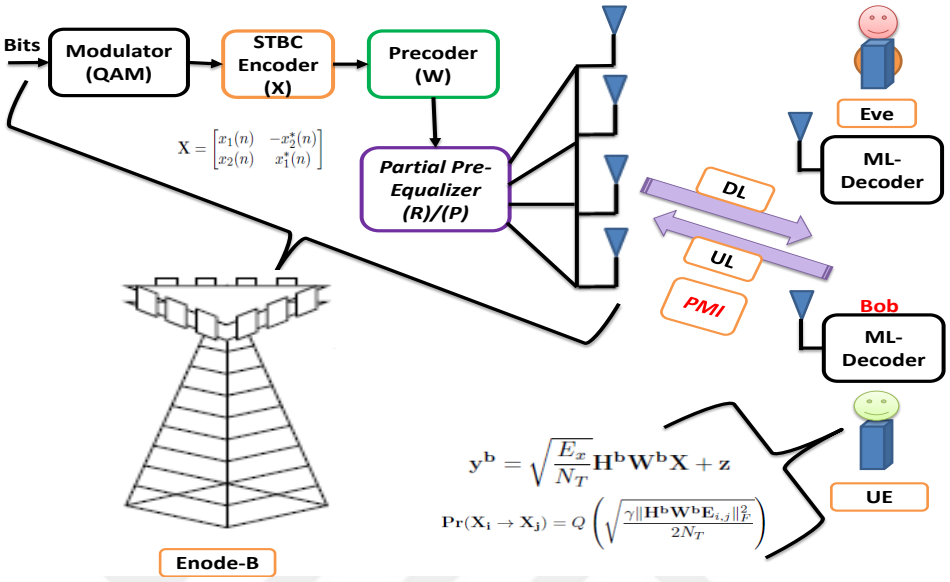


Figure 8.1: Precoded OSTBC model considered in this work.

Eve is given in (2) and (4) where $\mathbf{H^e}$ and $\mathbf{z^e}$ are the channel response, and AWGN of the channel of Eve, respectively.

$$\mathbf{y^b} = \sqrt{\frac{E_x}{N_T}}\mathbf{H^b W^b X} + \mathbf{z^b} = \sqrt{\frac{E_x}{N_T}}\mathbf{H^{bw} X} + \mathbf{z^b} \tag{8.1}$$

$$\mathbf{y^e} = \sqrt{\frac{E_x}{N_T}}\mathbf{H^e W^b X} + \mathbf{z^e} = \sqrt{\frac{E_x}{N_T}}\mathbf{H^{ew} X} + \mathbf{z^e} \tag{8.2}$$

In (1) and (2), E_x is the symbol energy, $\mathbf{N}_T$ is the number of transmit antennas, $\mathbf{H^b}$ is the channel realization of $\mathbf{N}_T$ transmit antennas, $\mathbf{W^b}$ is the optimal selected precoding matrix based on the legitimate user's channel. The process of selecting $\mathbf{W^b}$ will be discussed in the next section. $\mathbf{H^{bw}} \in C^{[1\times 2]}$ is the effective channel vector resulted from multiplying $\mathbf{H^b} \in C^{[1\times 4]}$ by $\mathbf{W^b} \in C^{[4\times 2]}$. Specifically, The entries of these matrices can be denoted as shown below:

$$\mathbf{H^{bw/ew}} = \mathbf{H^{b/e}}^{[1\times 4]} \times \mathbf{W^{b/e}}^{[4\times 2]} = \begin{bmatrix} h_1^{b/e}(n) & h_2^{b/e}(n) \end{bmatrix}.$$

Let $y_1^b(n)$ and $y_2^b(n)$ denote the received symbols at time t and $t+T_s$ respectively. Then (1) and (2) can be shown as

$$y_1^b(n) \quad = \quad h_1^b(n) * x_1(n) + h_2^b(n) * x_2(n) + z_1^b(n)$$

$$
\begin{aligned}
y_2^b(n) &= -h_1^b(n) * x_2^*(n) + h_2^b(n) * x_1^*(n) + z_2^b(n) && (8.3)\\
y_1^e(n) &= h_1^e(n) * x_1(n) + h_2^e(n) * x_2(n) + z_1^e(n) \\
y_2^e(n) &= -h_1^e(n) * x_2^*(n) + h_2^e(n) * x_1^*(n) + z_2^e(n). && (8.4)
\end{aligned}
$$

If we take the conjugation of the received signal at the second time slot and then multiply by the hermitian transpose of Bob's and Eve's equivalent channel vector ($\mathbf{H^{bw/ew}}$), we get the following input output relationship at the receiver side:

$$
\begin{bmatrix} \hat{y}_1^{b/e}(n) \\ \hat{y}_2^{b/e}(n) \end{bmatrix} = (|h_1^{b/e}(n)|^2 + |h_2^{b/e}(n)|^2) \begin{bmatrix} x_1(n) \\ x_2(n) \end{bmatrix} + \begin{bmatrix} \hat{z}_1^{b/e}(n) \\ \hat{z}_2^{b/e}(n) \end{bmatrix},
$$

where any variable with hat $\hat{}$ represents the original variable multiplied by the matrix

$$
\hat{H} = \begin{bmatrix} h_1^{*b/e}(n) & h_2^{b/e}(n) \\ h_2^{*b/e}(n) & -h_1^{b/e}(n) \end{bmatrix}.
$$

Accordingly, the maximum likelihood (ML) signal detection process at the receiver side is simplified as follows:

$$
\hat{\mathbf{X}}_{i,ML}^{\mathbf{b/e}} = \Phi \left(\frac{\hat{\mathbf{y}}_{\mathbf{i}}^{\mathbf{b/e}}(\mathbf{n})}{(|h_1^{b/e}(n)|^2 + |h_2^{b/e}(n)|^2)} \right), i = 1, 2, 3, ... \qquad (8.5)
$$

where $\Phi(.)$ represents a slicing function that performs a separable decoding process at the receiver. Moreover, since Eve is a passive node, we assume that Alice has no information about the CSI of Eve's channel $\mathbf{H^e}$. Additionally, channel reciprocity property is adapted in our proposed method, where downlink channel can be estimated from the uplink one. Besides, we assume that both Bob and Eve experience uncorrelated, independent channel realizations due to the fact that the wireless channel response is unique and special to the locations of the transmitter and receiver as well as the environment characteristics. Therefore, $\mathbf{H^b}$ and $\mathbf{H^e}$ are uncorrelated. This assumption coincides and matches with the practical situation where Eve's location cannot be exactly same as that of Bob.

8.3 Precoded OSTBC Method

As mentioned previously, many MIMO based physical security methods have been proposed in the literature. In spite of the effectiveness of such approaches, most of them suffer from sacrificing some of the precious communication resources such as transmission power. Generally, the source of security was based on using artificial noise, optimum power allocation, beam-forming, secret key generation, and antenna subset modulation. However, here in the first part of our study, we show that choosing an optimal precoding matrix from a codebook in such a way that pairwise error probability at Bob is minimized to the lowest possible level, can provide a secrecy gap region between Bob and Eve over all expected SNR values. It is very important to emphasize that the obtained security gain is achieved considering the worst security scenario, where Eve is capable of knowing the selected PMI. Although both Alice and Bob can use the estimated channel in implementing a similar selection process to choose the best PMI without feeding back any bits about the selected PMI, in current practical wireless systems such as LTE, PMI value is usually sent via publicly accessed channel to avoid the imperfect channel reciprocity problem. Consequently, Eve can detect the selected PMI, and then use it in the detection process.

In the following, the process of selecting optimal precoding matrix is explained and discussed [88]. Considering the precoded OSTBC described previously in the system model section, the space-time codeword $\mathbf{X}$ is first precoded by a special matrix $\mathbf{W}$ which is selected from an already designed codebook $\mathbf{G} = \{\mathbf{W}_1, \mathbf{W}_2, \mathbf{W}_3, ..., \mathbf{W}_T\}$. The purpose here is to select and pick an appropriate codeword that can improve the overall performance so that the error probability can be minimized to the lowest level possible. Since N_T channels stay unchanged during several consecutive codewords, the Bob's received signal $\mathbf{y^b} \in C^{[1\times T]}$ over T becomes

$$\mathbf{y^b} = \sqrt{\frac{E_x}{N_T}}\mathbf{H^b}\mathbf{W^b}\mathbf{X} + \mathbf{z}. \tag{8.6}$$

For a given channel $\mathbf{H^b}$ and precoder $\mathbf{W^b}$, the error probability of pairwise codeword is considered as $\mathbf{Pr}(\mathbf{X_i} \rightarrow \mathbf{X_j})$. This probability metric represents the

likelihood that $\mathbf{X_i}$ is send whereas $\mathbf{X_j}$ with $j \neq i$ is decoded. The expression of the pairwise error probability is formulated as [88]

$$\mathbf{Pr}(\mathbf{X_i} \rightarrow \mathbf{X_j}) = Q\left(\sqrt{\frac{\gamma\|\mathbf{H^b}\mathbf{W^b}\mathbf{E}_{i,j}\|_F^2}{2N_T}}\right), \tag{8.7}$$

where γ is the signal-to-noise ratio (SNR), given as $\gamma = \frac{Ex}{N0}$, $\mathbf{E}_{i,j}$ is the error matrix between $\mathbf{X_i}$ and $\mathbf{X_j}$ defined as $\mathbf{E}_{i,j} = \mathbf{X_i} - \mathbf{X_j}$, $\|.\|_F^2$ is the squared Frobenius norm, which physically computes the total power gain. From (7), it is evident that in order to minimize the pairwise error probability, the term $\|\mathbf{H^b}\mathbf{W^b}\mathbf{E}_{i,j}\|_F^2$ has to be maximized. This results in the following criterion for codeword selection

$$\begin{aligned} \mathbf{W}_{opt} &= \arg \max \|\mathbf{H^b}\mathbf{W^b}\mathbf{E}_{i,j}\|_F^2, \ \mathbf{W^b} \in \mathbf{G}, \ i \neq j \\ &= \arg \max \|\mathbf{H^b}\mathbf{W^b}\|_F^2, \ \mathbf{W^b} \in \mathbf{G}. \end{aligned} \tag{8.8}$$

Solving the corresponding optimization problem for arbitrary N_T, codeword length M, and codebook size L, (8) can be formulated into the famous Grassmannian packing problem as in [133]. However, since this solution is somehow sophisticated and not straightforward, it is very common in the literature to use another more efficient and realistic (but suboptimal) method called Discrete Fourier Transform (DFT) matrices. The codebook composed of the DFT matrices can be given as

$$\mathbf{G} = \left[\mathbf{W}_{DFT} \quad \theta\mathbf{W}_{DFT} \quad . \quad . \quad . \quad \theta^{L-1}\mathbf{W}_{DFT}\right].$$

The first precoding matrix $\mathbf{W}_{DFT}$ is taken by selecting M columns of $N_T \times N_T$ DFT matrix. Moreover, θ is the diagonal matrix obtained as

$$\theta = diag\left(\left[e^{j2\pi u_1/N_T} \quad e^{j2\pi u_2/N_T} \quad . \quad . \quad . \quad e^{j2\pi u_{N_T}/N_T}\right]\right)$$

with free design variables $\{u_i\}_{i=1}^{N_T}$ to be specified and determined. Assume the first precoding matrix $\mathbf{W}_{DFT}$ is given, the remaining (L-1) precoders can be calculated and obtained through multiplying $\mathbf{W}_{DFT}$ by $\theta_i, i = 1, 2, ...L-1$. Free variables $\{u_i\}_{i=1}^{N_T}$ are specified such that the minimum chordal distance is maximized as

$$\mathbf{u} = \arg \max_{\{u_1, .u_{N_T}\}} \min_{\{l=1,.N-1\}} d(\mathbf{W}_{DFT}, \theta^l \mathbf{W}_{DFT}). \tag{8.9}$$

As shown in the previous design equations, the selection process of the suboptimal precoding matrix is based on the channel response of the intended receiver (Bob), but not Eve's channel, which is independent of Bob's one. As a result, one can intuitively expect obtaining a secrecy gap region between Bob and Eve. This intuition is verified by simulation results that show the exact performance difference between Bob and Eve as it will be demonstrated in Section V, Fig. 8.2. It is worth mentioning that the main reason behind the enhancement in the BER performance of Bob compared to Eve is the increase in the effective received SNR. More precisely, SNR increased as a result of achieving orthogonal transmission among the parallel channels toward Bob through precoding. Accordingly, the average received SNR over each symbol becomes

$$\mathbf{SNR} = \frac{\gamma \|\mathbf{HW}\|_F^2}{M}. \tag{8.10}$$

8.4 Proposed PCPPE Method

In the previous method (POSTBC), it is noticed from Eve's BER performance (Fig. 8.2) that although there is a security gap between Bob and Eve at comparable SNRs, still there is a nontrivial amount of information leakage at Eve. In other words, Eve's good performance enables her to detect some information bits correctly. Consequently, the provided secrecy by POSTBC method alone is obviously limited, not reliable and might be insufficient in some cases, where higher security gap is extremely needed to ensure better confidentiality at any distance Eve may be located from the base station (BS). More accurately, if Eve is closer to the BS than Bob, then secure link is hard to be achieved. For instance, when the SNR value at Eve is 20 dB, while it is 10 dB at Bob, then Eve can decode the data better than Bob. This fact motivates finding a way to enhance the previous method so that better security performance (i.e. larger BER gap between Bob and Eve) can be achieved. Therefore, a hybrid technique that combines the use of precoded OSTBC along with partial pre-equalizing (PCPPE) is introduced.

In this method, a new modified precoder, that takes security requirements into account, is proposed. Particularly, besides exploiting the conventional precoding

process (explained in section 8.3), the transmitter designs a new precoder that exploits the knowledge of its estimated channel amplitudes or phases experienced by each antenna with respect to the trusted receiver. These estimates are gathered in the form of amplitude based vector as shown in (11) or phase based vector as shown in (12). Now, to enhance the security performance, one can think of converting the vector $\tilde{\mathbf{R}}$ to a diagonal matrix $\mathbf{R}$ and then multiply it with the original precoding matrix $\mathbf{W}$ to get an encrypted and equalized precoding matrix denoted as ($\mathbf{RW}$). In this case the transmitted symbols are precoded by ($\mathbf{RW}$) in stead of only $\mathbf{W}$. Since $\mathbf{R}$ is related to Bob's channel amplitudes, which are independent from those associated with Eve, a security performance gain is expected to occur.

However, although this direct method can acquire a good performance gain,

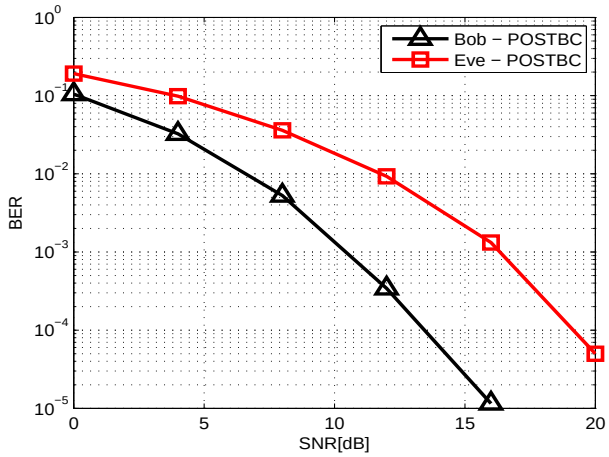


Figure 8.2: BER of POSTBC scheme for two streams (M=2) and $[4 \times 1]$ antenna system with 4QAM in a block Rayleigh fading channel. The selected PMI is assumed to be known by Eve (the worst security scenario).

it creates some serious problems regarding high power fluctuation and transmit power increase. To overcome these issues, while being still able to obtain a good security performance, we perform the following mathematical processing on one of the two created vectors $\tilde{\mathbf{R}}$ or $\tilde{\mathbf{P}}$ as both of them are related to Bob's condition but not Eve. For simplicity, let's just focus on $\tilde{\mathbf{R}}$ keeping in mind that the same processing can be applied on $\tilde{\mathbf{P}}$ as well. Hence, $\tilde{\mathbf{R}}$ is used as an input vector to a Singular Value Decomposition (SVD) process to get an orthogonal

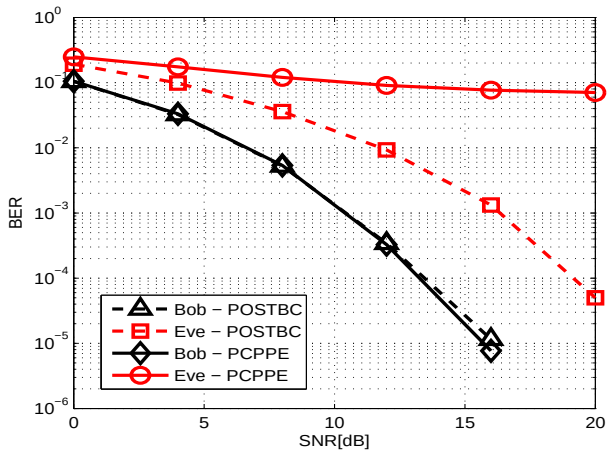


Figure 8.3: BER performance comparison between POSTBC and PCPPE methods with 4QAM modulation. Both the selected PMI and the employed security method are assumed to be known by Eve (the worst security scenario).

matrix called $\mathbf{F}$ as shown in (13). This process is used to overcome the aforementioned problems, more precisely, the power spectrum of $\tilde{\mathbf{R}}$ is collected in $\mathbf{E}$ (one singular value), while $\mathbf{U}$ is always a unity number. Therefore, both $\mathbf{E}$ and $\mathbf{U}$ can be dropped and only matrix $\mathbf{F}$ is taken. This matrix has several interesting properties: First, it is an orthogonal matrix with size of $(N_T \times N_T)$ and norm of unity. Second, its inverse is itself and its transpose is itself. Third, it maps the amplitude channel randomness to two dimensions instead of only one. As a result, $\mathbf{F}$ is used along with $\mathbf{W_{opt}}$ to constitute a new precoding matrix called $\mathbf{V}$ as shown in (14).

$$\tilde{\mathbf{R}} = \left[\frac{1}{|h^b 1|} \quad \frac{1}{|h^b 2|} \quad \frac{1}{|h^b 3|} \quad \cdots \quad \frac{1}{|h^b N_T|}\right] \tag{8.11}$$

$$\mathbf{R} = diag\left\{\left[\frac{1}{|h^b 1|} \quad \frac{1}{|h^b 2|} \quad \frac{1}{|h^b 3|} \quad \cdots \quad \frac{1}{|h^b N_T|}\right]\right\}$$

$$\tilde{\mathbf{P}} = \left[\frac{1}{\phi(h^{b1})} \quad \frac{1}{\phi(h^{b2})} \quad \frac{1}{\phi(h^{b3})} \quad \cdots \quad \frac{1}{\phi(h^{bN_T})}\right] \tag{8.12}$$

$$\mathbf{SVD} \quad \left\{\tilde{\mathbf{R}}\right\} = \mathbf{UEF'} \tag{8.13}$$

$$\mathbf{V} = \mathbf{FW_{opt}} \tag{8.14}$$

$$\mathbf{W_{opt}} = \arg \max \; Tr\left(\|\mathbf{HFW}\|_F^2\right), \; \mathbf{W} \in \mathbf{G} \tag{8.15}$$

$$\mathbf{y^b} = \sqrt{\frac{\mathbf{E}_x}{N_T}}\mathbf{H^b F^b W^b_{opt} X} + \mathbf{z^b} \tag{8.16}$$

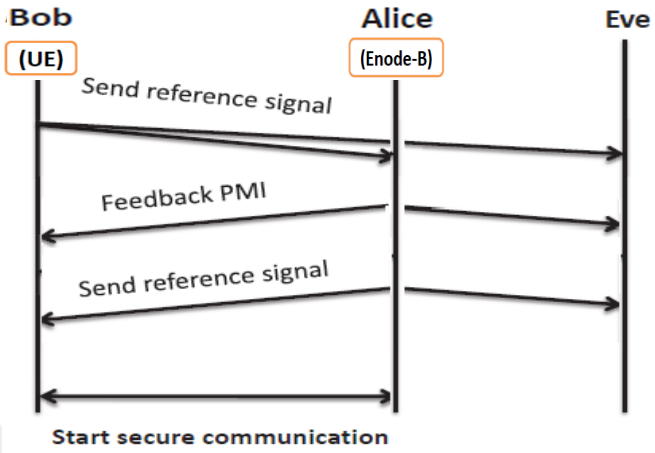


Figure 8.4: Signaling procedure of the proposed PCPPE method.

$$\mathbf{y^b} = \sqrt{\frac{\mathbf{E}_x}{N_T}}\mathbf{H^b}\mathbf{V_u^b}\mathbf{X} + \mathbf{z^b} = \sqrt{\frac{\mathbf{E}_x}{N_T}}\mathbf{H_u^{bvw}}\mathbf{X} + \mathbf{z^b} \tag{8.17}$$

$$\mathbf{y^e} = \sqrt{\frac{\mathbf{E}_x}{N_T}}\mathbf{H^e}\mathbf{V_u^b}\mathbf{X} + \mathbf{z^e} = \sqrt{\frac{\mathbf{E}_x}{N_T}}\mathbf{H_u^{evw}}\mathbf{X} + \mathbf{z^e} \tag{8.18}$$

Yet, another necessary modification is still needed to be performed. This new amendment is related to the traditional selection process of $\mathbf{W_{opt}}$. Previously, $\mathbf{W_{opt}}$ is chosen merely based on Bob's channel to minimize the pair-wise error probability. However, because of the modification that has been performed on the precoding process, the new selection should take into account the effect of $\mathbf{F^b}$ on the pair-wise probability as it becomes a kernel part of the precoding process, where it is specifically designed to meet security requirements. Otherwise, a performance degradation is going to happen. The new selection process is represented mathematically by (15), where $\mathbf{W_{opt}}$ is chosen based on both $\mathbf{H^b}$ and $\mathbf{F^b}$. After doing this modification along with avoiding the aforementioned problems, the secure communication is now ready to be started. Note that both the transmitter and receiver should be able to estimate and construct the effective channel vector $\mathbf{H_u^{bvw}}$ and use it properly to detect and decode the transmitted symbols. Fig. 8.4 summarizes the signaling procedure of the PCPPE scheme based on a practical MISO system with codebook-based precoding. As shown, the receiver (Bob) first sends out a reference signal to the transmitter (Alice) to estimate the channel matrix $\mathbf{H^b}$. The transmitter uses $\mathbf{H^b}$ to calculate $\mathbf{F^b}$ using SVD process,

then use it along with $\mathbf{H^b}$ in finding the PMI from the universal codebook $\mathbf{G}$ that maximizes the norm found in (15). Then, Alice sends out the selected PMI via a publicly accessed channel (i.e. Eve can detect the PMI), followed by sending another reference signal to Bob. Under the assumption of channel reciprocity, Alice and Bob are able to compute the same effective channel vector $\mathbf{H_u^{bvw}}$, but Eve is unable to obtain the same one since her channel is different than Bob's one. After this signaling process, secure communication starts.

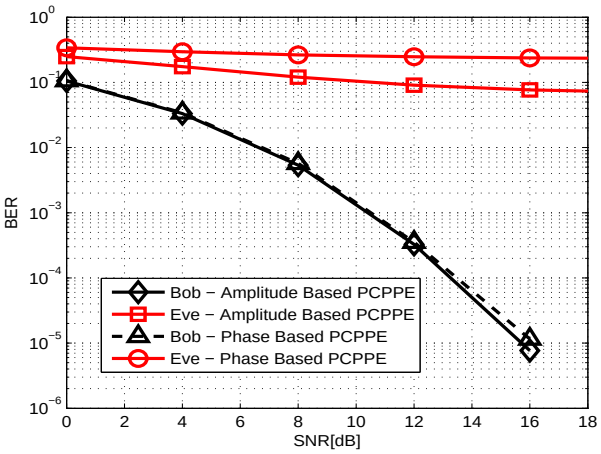


Figure 8.5: BER performance comparison between amplitude based PCPPE method and phase based PCPPE with 4QAM.

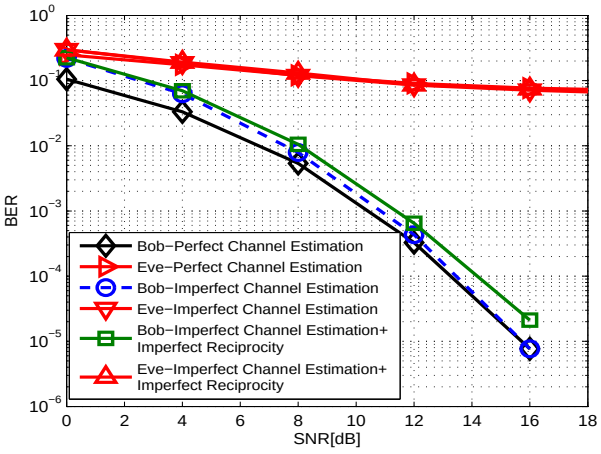


Figure 8.6: BER performance of PCPPE method with 4QAM under imperfect channel estimation and imperfect channel reciprocity.

8.5 Simulation Results

Since our proposed security scheme is based on signal processing, the effectiveness of the developed technique is characterized by BER performance verses average SNR. First, the codebook using the design method in [134], which is adopted in WiMAX wireless systems, is generated with the following parameters $N_T = 4$, $M = 2$, and $L = 64$. Then the BER performance of the precoded OSTBC with $N_T = 4$, $N_R = 1$ is simulated. Fig. 8.3 depicts a comparative BER performance between Bob and Eve in a block flat Rayleigh fading channel using QAM modulation considering two cases: the first case is with only POSTBC, which is also shown alone in Fig. 8.2, whereas the second is with PCPPE in which the original precoder is modified by the estimated channel amplitudes. It is obvious that there is a small security gap region in the first case (POSTBC). This gap is improved more by employing the modified precoder using PCPPE method. It is evident that the performance of Bob gets better, while it gets worse for Eve since her extracted new precoding matrix is different from Bob, whose channel is uncorrelated with Eve due to being in different location. By doing this, secure link has been assured at any distance Bob or Eve might be located from the BS. Fig. 8.5 shows that phase based PCPPE outperforms amplitude based PCPPE method, which is due to having different distributions for amplitude and phase. Amplitude has Rayleigh distribution, while phase has uniform distribution, in which the probability of occurrence of each event is the same (independent events), resulting in more randomness compared to amplitude based method. Fig. 8.6 exhibits the BER performance of PCPPE method under imperfect channel estimation (ICE) and imperfect channel reciprocity (ICR). ICE is modeled by introducing intentional errors according to the mean square error (MSE) values of a least square estimator (LSE). More accurately, the following equation is used $MSE = \Delta H = 10^{\frac{-SNR}{10}}$ at both the receiver and the transmitter. On the other hand, ICR is modeled by adding a constant value α, which is added to the estimated MSE value over all SNRs i.e. $MSE = \Delta H = 10^{\frac{-SNR}{10}} + \alpha$. In our simulation, α is considered to be 0.1. As depicted in Fig. 8.6, ICE and ICR lead to a small degradation due to the mismatch of the generated modified precoders at both sides. It is observed that ICE creates a decaying degradation in the

BER performance since MSE value at high SNR becomes very low, while ICR produces a constant degradation over all SNR since α is independent of SNR. However, this small degradation can be overcome by increasing the training sequence length, where better channel estimation can be obtained. In all of our simulation experiments, the worst security scenario is taken into account, where Eve is considered to be fully knowledgeable of the implemented security method as well as the selected PMI. This assumption is closer to the practical systems, in which PMI is fed back to the transmitter. Based on the obtained results and from both security and reliability perspectives, it is demonstrated that the security performance of PCPPE outperforms POSTBC scheme. This enhancement is achieved without sacrificing any of the precious resources such as spectral bandwidth or transmit power. Therefore, it is highly recommended to use PCPPE method for providing secure OSTBC-MISO systems in green wireless networks.

8.6 Conclusion

The security performance obtained by employing POSTBC in wireless networks has been investigated. The worst practical security scenario, where Eve has knowledge on the selected PMI is considered. The obtained results have depicted that there is a security gap region in the resulting BER performance as a consequence of using POSTBC. Moreover, the security performance is enhanced more by developing a new robust and hybrid security method called PCPPE, where the original precoder is re-designed to take security requirements into account. This method is performed without sacrificing any communication resources, thus it is considered to be a green and power efficient security technique that can be integrated with current and future wireless systems such as 4G and 5G.

Chapter 9

Conclusions and Future Research Directions

9.1 Concluding Remarks

To address the challenge of providing security against eavesdropping; novel, joint PHY/MAC layer security designs are developed and proposed for providing confidentiality against eavesdropping in current and future wireless networks. The conclusions drawn from the research studies conducted in this thesis can be summarized as follows:

I) ARQ as a MAC layer mechanism with MRC on a signal level as a physical layer mechanism, are capable of providing confidential wireless services for legitimate users against eavesdropping. Particularity, a tangible security gap in the PER (which is suggested to be used as a new practical security metric in cross layers security design) is observed. The obtained results are analyzed using PER, where the exact gap difference in PER between Bob and Eve is determined. Accurate PER formulas for both Eve and Bob in i.i.d Rayleigh fading channel are derived to determine the exact gap difference in PER between Bob and Eve. The

acquired simulation and theoretical results show that the employment of the proposed scheme can boost data security for certain services at specific SNR values, and it gets enhanced as number of allowable retransmissions (L) increases. Furthermore, QoS-based adaptive modulation is proposed to be used along with ARQ scheme to ensure security for specific services at any SNR Eve may encounter. Also, it has been shown that taking QoS requirements for different services into account during the design phase is an efficient way for providing secure wireless systems.

II) ARQ along with MRC and artificial noise have jointly been exploited to develop an eavesdropping-resilient system. This has been achieved by intentionally adding a properly well-designed channel amplitude-dependent, null-space-independent, PAPR-aware, and QoS-based (adaptive) artificial noise on top (superimposed in the power domain) of the transmitted data packets in such a way that the added artificial noise vectors cancel each other at only the legitimate receiver, while severely deteriorating Eve's performance. It has been shown that without exceeding the QoS requirements set by the current LTE standard, and without degrading PER performance of the legitimate user, perfect secure service transmission can be achieved. For some services such as voice and video, it is observed that secure transmission can be attained by just forcing Eve to operate below the determined QoS requirements (unsatisfied QoS for Eve). Thus, security is guaranteed without sharing a secret key, nor imposing any changes in the receiver structure, making it a very suitable candidate technique for future 5G and beyond wireless networks as well as for low complexity Internet of Thing (IoT) devices. Besides, the proposed scheme is shown to help reduce the PAPR and OOBE of OFDM-based waveforms, resulting in a multi-purpose design.

III) An efficient 5G URLLC-tailored physical layer security technique, which can provide two security levels in TDD mode and one in FDD mode, has been proposed for protecting OFDM-based waveforms against eavesdropping. This transmission mechanism, which performs channel-based adaptive subcarrier selection and adaptive interleaving, results not only in providing remarkable secrecy gap, but also enhances the reliability performance of the legitimate user compared to the standard OFDM transmission. Moreover, the technique saves power and

provides secrecy even in the worst security scenario, where the eavesdropper is assumed to know the channel of the legitimate link due to using some kind of explicit FDD-based feedback. The presented results have proven the capability of the proposed scheme in achieving practical secrecy without increasing the complexity of the OFDM structure or knowing Eve's channel, making it very suitable for low complexity 5G-URLLC services (IoT-based remote control and tactile applications). Besides, a novel secure channel calibration technique is proposed to overcome the problem of having channel reciprocity mismatch between uplink and downlink transmissions.

VI) A CP-less OFDM design that eliminates the need of using excessive CPs between OFDM symbols is proposed. The design is shown to increase the spectral and power efficiency, reduce latency, and improve physical layer security while maintaining low receiver complexity, making it a strong candidate for meeting the requirements of future 5G and beyond services and applications. Particularly, a novel power domain-based method that removes the requirement of CP while keeping the whole detection process the same at the receiver side is achieved by using a special design of alignment signals. These signals are added in the power domain of the transmitted OFDM symbols in order to achieve two goals simultaneously: 1) removing the inter-symbol-interference between symbols and 2) making the signal circular at the receiver side. Simulation results showed that spectral and power efficiency got enhanced, latency got reduced, and secrecy got improved while maintaining low complexity equalization at the Rx side.

V) An inherently secure 5G waveform design for providing physical security over dispersive channels has been developed. Particularly, orthogonal basis functions, whose time and frequency characteristics are different from those of Fourier-based ones, are extracted from the legitimate channel and then used as data bearing carriers instead of the exponential functions in OFDM. Thus, channel-based transformations are used instead of Fourier transforms to diagonalize the channel response of only the legitimate receiver. Besides security, the scheme is shown to enhance reliability, power efficiency and robustness against channel impairments.

IV) It has been observed that the usage of PMI in precoded OSTBC wireless

systems can result in a noticeable secrecy gap. Moreover, the security performance is enhanced more by developing a new robust and hybrid security method called PCPPE, where the original precoder is re-designed to take security requirements into account. This method is performed without sacrificing any communication resources, thus it is considered to be a green and power efficient security technique that can be integrated with current and future wireless systems such as 4G and 5G.

9.2 Challenges, Recommendations and Future Research Directions

1. Based on the aforementioned material we have presented and specifically the block diagrams (Fig. 2.3 and Fig. 2.4) that concisely summarize the advantages and disadvantages of the existing physical layer security techniques and their branches, one can simply conclude that each security track and approach has its own Pros. (merits) and Cons (demerits). In particular, what may be suitable for some applications, systems, scenarios, and channel conditions might not be good for others. Thus, based on these substantial inferences and results, which have been made possible due to the security framework we carefully structured and offered, we can favor one method over another according to the our needs and requirements. Since each direction and each method has some promising security advantages in one side and some flaws as well in the other side, it is worth devoting some of our research efforts on developing new advanced security methods that are capable of minimizing the drawbacks/side effects of these security tracks and maximizing their merits. This goal can be attained through designing practical techniques which can help not only in security, but also satisfy the other communication system requirements such as reliability, complexity, power efficiency, spectral efficiency, delay and complexity. It is firmly anticipated that any technique adopts this approach will certainly make it interesting for both research and industry communities.

2. Another futuristic and promising research area, which is not yet investigated heavily in the literature, is cross layer security design such as cross MAC/PHY layer security, cross NET/PHY layer security, cross NET/MAC/PHY layer security, etc. These new security approaches aim at involving the upper-layers such as MAC and network layers in the physical security design process. This target can be achieved through exploiting the functionalities and mechanisms of these layers for security purposes. For example, the degree of freedom existing in ARQ as a MAC layer mechanism along with maximal ratio combination, adaptive modulation, artificial noise, and other techniques as physical layer mechanisms can be adopted for security.

3. Adaptation processes including channel-based adaptive precoding, partial pre-equalization, optimized waveforms, adjustable filtering, resource allocation, parameters optimization and joint structural design of transmitters and receivers based on the channel between them (i.e., channel-based preprocessing and post-processing), are expected to dominate the design principle of future wireless networks because adaptive designs not only enhance the efficiency and performance of legitimate receivers, but also increases the security level of our systems. This is very applicable especially if we know some pre-information about the statistics of the malicious eavesdroppers and the specific spatial regions that we want our communication to be secure in. In spite of the many advantages that adaptation-based techniques offer, they are unfortunately not sufficient enough in scenarios where many eavesdroppers can collaborate and multiple different observations of the transmitted signal can be acquired from many spatial locations by Eve. Thus, a promising direction can be the integration of adaptation-based approaches with other security techniques (e.g., artificial noise) in order to maintain an adequate secrecy level against multiple eavesdroppers' cooperation and colluding while keeping the inherent merits of the adaptation-based approaches.

4. Cognitive security is another promising new research direction: In [135], authors proposed a novel concept of cognitive security (CS) for wireless communication that can provide adaptive, reliable, robust and comprehensive security solutions for wireless communication. In CS, physical layer security concept is exploited in a unique way, such that the radio first detects and combines the information from environmental conditions and radio channel. Afterwards, based on detected information, it detects the respective context. After detecting the context, radio adapts different propagation characteristics and takes necessary precautions to provide security.

5. Since most of the physical security techniques are completely based on exploiting the characteristics of the channel and its availability at both the transmitter and receiver sides, robust channel estimation along with reciprocity calibration becomes inevitable challenging task to encounter as it is difficult to achieve in practice. Thus, the effect of imperfect channel estimation and reciprocity mismatch should be taken into account when a new security method is designed to make sure that it is robust against these drawbacks; and in case it is not, then efficient practical channel calibration solutions are needed to tackle these issues. Additionally, although most of the aforementioned security directions consider somewhat the practical assumption of the fact that Bob's channel is independent of Eve in a wireless environment, which can be satisfied when they are separated apart by at least half a wavelength; this is still not always true, where there are cases and specific poor scattering environments where there might be a strong correlation between Bob and Eve [136]. In this case, the level of physical layer security will reduce significantly (e.g., secrecy will be exactly zero if both Bob and Eve are placed extremely close to each other). Thus, re-examining and investigating the existing physical layer security techniques under these conditions may give new insights about the practicality and robustness levels of the current available security methods.

6. For channel-based secret key generation approach, extracting keys with high rates remains a very challenging task, especially for poor scattering or line of site (LOS) environments, where there is no much randomness or variations

in the channel due to having long coherence time. To address this challenge, a few recent studies in the literature [137–142] have proposed creating virtual random channel [137] (by using opportunistic randomized beamforming [143] along with diversity) or by producing artificial interference [138] that can be used to generate high secret key rates with good entropy independent of the actual mobility and variations of the channel. Due to the practicality and super benefits provided by this channel-independent secret key generation approach [144], it is foreseen that more research studies and works related to deep performance analysis, investigation and practical implementation are needed in order to verify and validate the applicability of this approach for integration and extensions to other wireless systems and scenarios.

7. The effect of the pre-coding and artificial noise-based security techniques on the peak to average power ratio (PAPR), which is associated with power amplifier non-linearity problem, is mostly forgotten in the literature of physical layer security. Particularly, there are very little works about this practical important issue, which is so critical to a level that it may impede and even prohibit the applicability of many of the artificial noise-based security techniques in realistic situations. Thus, such serious practical issues should be examined for all the previously provided physical layer security techniques via revisiting them from a different perspective in order to test and investigate whether these security techniques cause PAPR increase or not; and if they do, then efficient signal processing techniques need to be designed in order to provide proper solutions to this problem. In the meanwhile, researchers, who are developing new security algorithms are strongly recommended to take such an issue into account while designing their security schemes. In [145], the researchers showed that the famous artificial noise based technique proposed by Nagi and Goel in [48] creates high PAPR similar to that produced by an OFDM signal due to the accidental in-phase addition (superposition) of AN subspaces and the data subspaces. To mitigate the PAPR of the transmitted signal, an angle rotation based technique was proposed to reduce the PAPR, while maintaining the same secrecy capacity performance as that of the original artificial noise aided method.

In [146], the authors proposed to either change the distribution of the added AN from Gassuain to uniform in flat fading environments or to use an optimized AN that not only avoids PAPR increase but also help reduce the PAPR of OFDM signal transmission over frequency selective channels (i.e., time dispersive channel).

8. There are some extremely challenging security scenarios such as those related to line of site (LOS) environments and the eavesdropper is located within the same direction of the legitimate user. In this case, many of the physical layer security techniques such as conventional linear beamforming [27, 147, 148], classical antenna subset modulation [149], directional modulation [150], artificial noise-based MIMO techniques [48], etc. will fail to provide security. Generally speaking, there is a huge need to design much more practical PLS techniques that can sustain its applicability in scenarios of poor scattering (non-fading), static time invariant (non-dynamic), or non-dispersive channels (no multipath), where most of the existing security techniques that exploit the opposite of these scenarios may not be able to provide physical security.

9. The joint optimal design of secrecy, reliability, throughput, delay and the trade-off among them is another important area, which is not yet well investigated in the literature. In general, providing physical secrecy constraints usually come at the expense of compromising other system requirements. For example, channel coding-based techniques sacrifice spectral efficiency, while artificial noise-based techniques compromise power efficiency, where unnecessary power is transmitted in this case. Thus, an optimal design that takes the quality of service requirements such as delay, throughput, and packet error rate into account while insuring security, is an essential track in future research security work, Recent work has shown that the previous knowledge of the type of running application (service) at user side is a very advantageous feedback that should be taken into account during the phase of security design process to ensure conveying a certain service confidentially. The reason for this is that, when we get to know the application run by the legitimate user, we adopt our transmission parameters exactly

according to user needs, no more no less, while these parameters ensure in the same time that Eve is operating below these requirements making it difficult for her to get the required QoS. Interestingly, this kind of security design approaches states that strong secrecy is not always needed to provide a perfect secure service.

10. Most of the PLS techniques and approaches whether they are key-based (Shannon's model) or key-less (Wyner's model) are basically designed to merely secure messaging service without considering the actual required security level of other types of used services such as voice, video, VOIP, streaming, gaming, URLLC, mMTC, etc. For this kind of services, the ultimate goal is to deliver them to the users reliably and within the determined and standardized Quality of Service (QoS) requirements. In such a situation, it is anticipated that perfect secrecy (i.e., perfectly zero information leakage to Eve) is not always needed to provide a perfectly secure service. In reality, each service has different QoS requirements than the others, and if we ensure that Eve is operating below these requirements, then practical service-based secrecy can be guaranteed. Thus, a promising research direction would be to redesign the existing PLS techniques from a much more practical perspective where the actual QoS requirements of real services such as URLLC, mMTC, VOIP, video, etc. are taken into account.

11. Last but not least, designing hybrid security techniques which can provide more than one level of security, i.e., two levels (sources) of security: one is coming from an SINR-based technique, while the other is coming either from a complexity-based technique or from conventional cryptographic based techniques. This will help make the security scheme more robust and immune against eavesdropping.

Bibliography

[1] 3GPP, "Policy and charging control architecture," 2012.

[2] N. Yang, M. Elkashlan, T. Duong, J. Yuan, and R. Malaney, "Optimal Transmission with Artificial Noise in MISOME Wiretap Channels," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, pp. 1–1, 2015.

[3] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, oct 1949.

[4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, oct 1975.

[5] Y.-S. Shiu, S. Chang, H.-C. Wu, S. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Commun.*, vol. 18, pp. 66–74, apr 2011.

[6] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tuts.*, vol. 16, pp. 1550–1573, jan 2014.

[7] Y. Liu, H. H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surv. Tutorials*, vol. 19, pp. 347–376, First quarter 2017.

[8] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. of the IEEE*, vol. 104, pp. 1727–1765, Sept 2016.

[9] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. of the National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, 2017.

[10] M. Bloch and J. Barros, *Physical-layer security: From information theory to security engineering*. Cambridge University Press, Aug. 2008.

[11] R. Liu and W. Trappe, *Securing wireless communications at the physical layer*. Springer, 2010.

[12] X. Zhou, L. Song, and Y. Zhang, *Physical layer security in wireless communications*. CRC Press Taylor and Francis Group, 2013.

[13] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, *Signal processing approaches to secure physical layer communications in multi-antenna wireless systems*. New York, NY, USA: Springer, 2014.

[14] M. Baldi and S. Tomasin, *Physical and data-link security techniques for future communication systems*. 1876-1100, Springer International Publishing, 2016.

[15] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Sig. Process. Mag.*, vol. 30, pp. 41–50, Sep 2013.

[16] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Sig. Process. Mag.*, vol. 30, pp. 16–28, Sep 2013.

[17] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proc. IEEE*, vol. 103, pp. 1725–1746, Oct 2015.

[18] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Commun. Surv. Tuts.*, vol. 17, no. 2, pp. 1023–1043, 2015.

[19] C. Shahriar, M. La Pan, M. Lichtman, T. C. Clancy, R. McGwier, R. Tandon, S. Sodagari, and J. H. Reed, "Phy-layer resiliency in OFDM communications: A tutorial," *IEEE Commun. Surv. Tuts.*, vol. 17, no. 1, pp. 292–314, 2015.

[20] X. Chen, C. Zhong, C. Yuen, and H.-H. Chen, "Multi-antenna relay aided wireless physical layer security," *IEEE Commun. Mag.*, vol. 53, pp. 40–46, Dec 2015.

[21] E. Jorswieck, S. Tomasin, and A. Sezgin, "Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing," *Proc. IEEE*, vol. 103, pp. 1702–1724, Oct 2015.

[22] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surv. Tuts.*, vol. 19, pp. 1027–1053, Secondquarter 2017.

[23] A. Hyadi, Z. Rezki, and M. S. Alouini, "An overview of physical layer security in wireless communication systems with CSIT uncertainty," *IEEE Access*, vol. 4, pp. 6121–6132, 2016.

[24] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[25] Z. E. Ankarali, Q. H. Abbasi, A. F. Demir, E. Serpedin, K. Qaraqe, and H. Arslan, "A comparative review on the wireless implantable medical devices privacy and security," in *2014 4th Int. Conf. on Wireless Mob. Commun. and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH)*, pp. 246–249, Nov 2014.

[26] M. H. Yilmaz and H. Arslan, "A survey: Spoofing attacks in physical layer security," in *2015 IEEE 40th Local Comput. Networks Conf. Work. (LCN Work.)*, pp. 812–817, oct 2015.

[27] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized

artificial-aoise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, 2011.

[28] M. Li, S. Kundu, D. A. Pados, and S. N. Batalama, "Waveform design for secure SISO transmissions and multicasting," *IEEE J. Sel. Areas Commun.*, vol. 31, pp. 1864–1874, sep 2013.

[29] H. Reboredo, J. Xavier, and M. R. D. Rodrigues, "Filter design with secrecy constraints: The MIMO gaussian wiretap channel," *IEEE Trans. Signal Process.*, vol. 61, no. 15, pp. 3799–3814, 2013.

[30] A. Subramanian, A. T. Suresh, S. Raj, A. Thangaraj, M. Bloch, and S. McLaughlin, "Strong and weak secrecy in wiretap channels," in *2010 6th Int. Symp. on Turbo Codes Iterative Inf. Process.*, pp. 30–34, IEEE, Sep 2010.

[31] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2515–2534, Jun 2008.

[32] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Commun. Lett.*, vol. 17, pp. 1483–1486, jul 2013.

[33] J. M. Hamamreh, M. Yusuf, T. Baykas, and H. Arslan, "Cross MAC/PHY layer security design using ARQ with MRC and adaptive modulation," in *IEEE Wireless Commun. and Netw. Conf., WCNC 2016, Doha, Qatar, April 3-6, 2016*, pp. 1–7, 2016.

[34] K. Morrison and D. Goeckel, "Secrecy rate pair constraints for secure throughput," in *IEEE Mil. Commun. Conf. (MILCOM)*, pp. 479–484, oct 2014.

[35] B. He, X. Zhou, and A. L. Swindlehurst, "On secrecy metrics for physical layer security over quasi-static fading channels," *IEEE Trans. Wireless Commun.*, vol. 15, pp. 6913–6924, Oct 2016.

[36] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451–456, Jul 1978.

[37] M. R. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Trans. Inf. Theory*, vol. 59, pp. 8077–8098, Dec 2013.

[38] E. Guvenkaya, J. M. Hamamreh, and H. Arslan, "On physical-layer concepts and metrics in secure signal transmission," *Phy. Commun.*, vol. 25, pp. 14 – 25, Aug. 2017.

[39] C. Liu, L. L. Yang, and W. Wang, "Secure spatial modulation with a full-duplex receiver," *IEEE Wireless Commun. Lett.*, vol. PP, no. 99, pp. 1–1, 2017.

[40] Z. Mheich, M. L. Treust, F. Alberge, P. Duhamel, and L. Szczecinski, "Rate adaptive secure HARQ protocol for block-fading channels," in *2014 22nd European Sig. Process. Conf. (EUSIPCO)*, pp. 830–834, Sept 2014.

[41] M. Le Treust, L. Szczecinski, and F. Labeau, "Secrecy and rate adaptation for secure HARQ protocols," in *2013 IEEE Inf. Theory Work.*, pp. 1–5, IEEE, Sep 2013.

[42] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure Hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, pp. 1575–1591, Apr 2009.

[43] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, pp. 883–894, Jun 2012.

[44] S. Tomasin and N. Laurenti, "Secure HARQ with multiple encoding over block fading channels: channel set characterization and outage analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, pp. 1708–1719, Oct 2014.

[45] C. W. Wong, J. M. Shea, and T. F. Wong, "Secret sharing in fast fading channels based on reliability-based hybrid ARQ," in *MILCOM 2008 - 2008 IEEE Military Commun. Conf.*, pp. 1–7, Nov 2008.

[46] C. D. T. Thai, J. Lee, and T. Q. S. Quek, "Physical-layer secret key generation with colluding untrusted relays," *IEEE Trans. Wirel. Commun.*, vol. 15, no. 2, pp. 1517–1530, 2016.

[47] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secret key generation using channel quantization with SVD for reciprocal MIMO channels," in *2016 Int. Symp. Wirel. Commun. Syst.*, pp. 597–602, IEEE, sep 2016.

[48] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, jun 2008.

[49] E. Guvenkaya and H. Arslan, "Secure communication in frequency selective channels with fade-avoiding subchannel usage," in *2014 IEEE Int. Conf. Commun. Work. ICC 2014*, pp. 813–818, IEEE, jun 2014.

[50] H. Qin, Y. Sun, T.-H. Chang, X. Chen, C.-Y. Chi, M. Zhao, and J. Wang, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Wireless Commun.*, vol. 12, pp. 2717–2729, Jun 2013.

[51] Z. E. Ankarali and H. Arslan, "Cyclic feature suppression for physical layer security," *Physical Communication*, pp. –, 2016.

[52] J. M. Hamamreh and H. Arslan, "Secure orthogonal transform division multiplexing (OTDM) waveform for 5G and beyond," *IEEE Commun. Lett.*, vol. 21, pp. 1191–1194, May 2017.

[53] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Secure pre-coding and post-coding for OFDM systems along with hardware implementation," in *13th Int. Wireless Commun. and Mobile Comput. Conf., IWCMC 2017, Valencia, Spain, Jun., 26-30, 2017*, pp. 1338–1343, 2017.

[54] J. Choi, "On channel-aware secure HARQ-IR," *IEEE Trans. Info. Foren. Sec.*, vol. 12, pp. 351–362, Feb 2017.

[55] S. Kundu, D. A. Pados, and S. N. Batalama, "Hybrid-ARQ as a communications security measure," in *ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc.*, pp. 5681–5685, IEEE, may 2014.

[56] J. M. Hamamreh, E. Güvenkaya, T. Baykas, and H. Arslan, "A practical physical-layer security method for precoded OSTBC-based systems," in

IEEE Wireless Commun. Netw. Conf., WCNC 2016, Doha, Qatar, Apr., 3-6, pp. 1–6, 2016.

[57] H. Mukhtar, A. Al-Dweik, M. Al-Mualla, and A. Shami, "Low complexity power optimization algorithm for multimedia transmission over wireless networks," *IEEE J. Sel. Topics in Signal Processing*, vol. 9, pp. 113–124, Feb 2015.

[58] S. Ge, Y. Xi, S. Huang, and J. Wei, "Packet error rate analysis and power allocation for CC-HARQ over rayleigh fading channels," *IEEE Commun.Letters*, vol. 18, pp. 1467–1470, Aug 2014.

[59] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE J. Sel. Areas in Commun.*, vol. 29, pp. 2067–2076, December 2011.

[60] D. Wang, P. Ren, Q. Du, Y. Wang, and L. Sun, "Secure cooperative transmission against jamming-aided eavesdropper for ARQ based wireless networks," *IEEE Access*, vol. PP, no. 99, pp. 1–1, 2017.

[61] T. V. K. Chaitanya and E. G. Larsson, "Optimal power allocation for hybrid ARQ with chase combining in i.i.d. rayleigh fading channels," *IEEE Trans. Commun.*, vol. 61, pp. 1835–1846, May 2013.

[62] J. M. Hamamreh, E. Basar, and H. Arslan, "OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services," *IEEE Access*, vol. 5, pp. 25863–25875, 2017.

[63] S. Liu, Y. Hong, and E. Viterbo, "Unshared secret key cryptography," *IEEE Trans. Wirel. Commun.*, vol. 13, pp. 6670–6683, dec 2014.

[64] C. Y. Wu, P. C. Lan, P. C. Yeh, C. H. Lee, and C. M. Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," *IEEE J. Sel. Areas Commun.*, vol. 31, pp. 1687–1700, Sep. 2013.

[65] A. Tom, A. Sahin, and H. Arslan, "Suppressing alignment: joint PAPR and out-of-band power leakage reduction for OFDM-based systems," *IEEE Trans. Commun.*, vol. 64, pp. 1100–1109, March 2016.

[66] Z. Ankarali, B. Pekoz, and H. Arslan, "Flexible radio access beyond 5G: A future projection on waveform, numerology frame design principles," *IEEE Access*, vol. PP, pp. 1–1, May 2017.

[67] H. Li, X. Wang, Y. Zou, and W. Hou, "Eavesdropping-Resilient OFDM System Using CSI-Based Dynamic Subcarrier Allocation," in *2013 IEEE 77th Veh. Technol. Conf. (VTC Spring)*, pp. 1–5, IEEE, jun 2013.

[68] Y. El Hajj Shehadeh, O. Alfandi, and D. Hogrefe, "Towards robust key extraction from multipath wireless channels," *J. Commun. Networks*, vol. 14, pp. 385–395, Aug 2012.

[69] H. Li, X. Wang, and J.-Y. Chouinard, "Eavesdropping-resilient OFDM system using sorted subcarrier interleaving," *IEEE Trans. Wireless Commun.*, vol. 14, pp. 1155–1165, Feb 2015.

[70] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation for secure OFDMA systems," *IEEE Trans. Veh. Technol.*, vol. 61, pp. 2572–2585, Jul. 2012.

[71] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Enhancing physical layer security of OFDM-based systems using channel shortening," in *Proc. 2017 IEEE Intern. Symp. Pers., Indoor, Mob. Radio Commun. (PIMRC)*, pp. 8–13, Oct. 2017.

[72] M. Yusuf and H. Arslan, "Enhancing physical-layer security in wireless communications using signal space diversity," in *MILCOM - 2016 IEEE Milit. Commun. Conf.*, pp. 1190–1194, Nov 2016.

[73] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Secure beamforming in downlink MISO non-orthogonal multiple access systems," *IEEE Trans. Veh. Technol.*, vol. 66, pp. 7563–7567, Aug 2017.

[74] 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," *IEEE Communications Magazine*, vol. 53, pp. 19–25, Dec 2015.

[75] M. Yusuf and H. Arslan, "On signal space diversity: An adaptive interleaver for enhancing physical layer security in frequency selective fading channels," *Physical Communication*, vol. 24, pp. 154 – 160, 2017.

[76] E. Basar, U. Aygolu, E. Panayirci, and H. V. Poor, "Orthogonal frequency division multiplexing with index modulation," *IEEE Trans. Sig. Processing*, vol. 61, pp. 5536–5549, Nov 2013.

[77] E. Basar, M. Wen, R. Mesleh, M. D. Renzo, Y. Xiao, and H. Haas, "Index modulation techniques for next-generation wireless networks," *IEEE Access*, vol. 5, pp. 16693–16746, Sep. 2017.

[78] E. Basar, "Index modulation techniques for 5G wireless networks," *IEEE Commun. Mag.*, vol. 54, pp. 168–175, July 2016.

[79] S.-W. Lei and V. K. N. Lau, "Performance analysis of adaptive interleaving for OFDM systems," *IEEE Trans. Veh. Tech.*, vol. 51, pp. 435–444, May 2002.

[80] R. W. Heath and A. Paulraj, "Antenna selection for spatial multiplexing systems based on minimum error rate," in *Proc. IEEE Int. Conf. Commun. Conf.*, vol. 7, pp. 2276–2280, 2001.

[81] C. S. Park and K. B. Lee, "Statistical multimode transmit antenna selection for limited feedback MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 4432–4438, Nov. 2008.

[82] M. Huemer, C. Hofbauer, and J. B. Huber, "The potential of unique words in OFDM," in *Proc. 15th Int. OFDM-Workshop 2010 (InOWo' 10)*, pp. 140–144, Sep. 2010.

[83] Z. Wang, R. F. Schaefer, M. Skoglund, H. V. Poor, and M. Xiao, "Strong secrecy for interference channels from channel resolvability," in *2015 49th*

Asilomar Conference on Signals, Systems and Computers, pp. 559–563, Nov 2015.

[84] A. Wickramasooriya, I. Land, and R. Subramanian, "Comparison of equivocation rate of finite-length codes for the wiretap channel," in *SCC 2013; 9th International ITG Conference on Systems, Communication and Coding*, pp. 1–6, Jan 2013.

[85] Z. E. Ankaral, M. Karabacak, and H. Arslan, "Cyclic Feature Concealing CP Selection for Physical Layer Security," in *2014 IEEE Military Communications Conference*, pp. 485–489, Oct 2014.

[86] M. K. Simon and M.-S. Alouini, *Fading Channel Characterization and Modeling*, pp. 15–30. John Wiley & Sons, Inc., 2002.

[87] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products P.891 (8.258)*. Academic, 7th edition ed., 2007.

[88] Y. Cho, J. Kim, W. Yang, and C. Kang, *MIMO-OFDM Wireless Communication with MATLAB*. Singapore: Wiley, Nov. 2010.

[89] S. Weinstein and P. Ebert, "Data transmission by frequency-division multiplexing using the discrete Fourier transform," *IEEE Trans. Commun. Tech.*, vol. 19, pp. 628–634, October 1971.

[90] A. A. Zaidi, R. Baldemair, H. Tullberg, H. Bjorkegren, L. Sundstrom, J. Medbo, C. Kilinc, and I. D. Silva, "Waveform and numerology to support 5G services and requirements," *IEEE Commun. Mag.*, vol. 54, pp. 90–98, November 2016.

[91] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE Access*, vol. 3, pp. 1206–1232, 2015.

[92] S. K. Chronopoulos, G. Tatsis, V. Raptis, and P. Kostarakis, "Enhanced PAPR in OFDM without deteriorating BER performance," *International Journal of Communications, Network and System Sciences*, vol. 4, pp. 164–169, Mar. 2011.

[93] S. K. Chronopoulos, V. Christofilakis, G. Tatsis, and P. Kostarakis, "Reducing peak-to-average power ratio of a turbo coded OFDM," *Wireless Engineering and Technology*, vol. 3, pp. 195–202, Oct. 2012.

[94] J. M. Hamamreh and H. Arslan, "Time-frequency characteristics and PAPR reduction of OTDM waveform for 5G and beyond," in *2017 10th Inter. Conf. Elect. Elect. Eng. (ELECO)*, pp. 681–685, Nov 2017.

[95] E. Gvenkaya, J. M. Hamamreh, and H. Arslan, "On physical-layer concepts and metrics in secure signal transmission," *Physical Communication*, vol. 25, no. Part 1, pp. 14 – 25, 2017.

[96] H. J. H. Yu, H.; Lee, "What is 5G? emerging 5G mobile services and network requirements.," *Sustainability*, vol. 9, no. 1848, 2017.

[97] C. Bockelmann, N. Pratas, H. Nikopour, K. Au, T. Svensson, C. Stefanovic, P. Popovski, and A. Dekorsy, "Massive machine type communications in 5G: physical and MAC layer solutions," *IEEE Commun. Mag.*, vol. 54, pp. 59–65, September 2016.

[98] P. J. W. Melsa, R. C. Younce, and C. E. Rohrs, "Impulse response shortening for discrete multitone transceivers," *IEEE Trans. Commun.*, vol. 44, pp. 1662–1672, Dec 1996.

[99] T. Karp, M. J. Wolf, S. Trautmann, and N. J. Fliege, "Zero-forcing frequency domain equalization for DMT systems with insufficient guard interval," in *Acoustics, Speech, and Signal Processing, 2003. Proceedings. (ICASSP '03). 2003 IEEE Inter. Conf.*, vol. 4, pp. IV–221–4 vol.4, April 2003.

[100] X.-G. Xia, "Precoded and vector OFDM robust to channel spectral nulls and with reduced cyclic prefix length in single transmit antenna systems," *IEEE Trans. Commun.*, vol. 49, pp. 1363–1374, Aug 2001.

[101] N. Kim, J. Ahn, O. S. Shin, and K. B. Lee, "Precoding design for cyclic prefix overhead reduction in a MISO-OFDM system," *IEEE Wireless Commun. Lett.*, vol. 6, pp. 578–581, Oct 2017.

[102] T. Taheri, R. Nilsson, and J. van de Beek, "Asymmetric transmit-windowing for low-latency and robust OFDM," in *2016 IEEE GC Wkshps*, pp. 1–6, Dec 2016.

[103] J. Lorca, "Cyclic prefix overhead reduction for low-latency wireless communications in OFDM," in *2015 IEEE 81st Vehic. Tech. Conf. (VTC Spring)*, pp. 1–5, May 2015.

[104] X. Wang, Y. Wu, J. Y. Chouinard, and H.-C. Wu, "On the design and performance analysis of multisymbol encapsulated OFDM systems," *IEEE Trans. Veh. Tech.*, vol. 55, pp. 990–1002, May 2006.

[105] K. Arya and C. Vijaykumar, "Elimination of cyclic prefix of OFDM systems using filter bank based multicarrier systems," in *TENCON 2008 - 2008 IEEE Region 10 Conf.*, pp. 1–5, Nov 2008.

[106] K. Hueske and J. Gotze, "Ov-OFDM: A reduced PAPR and cyclic prefix free multicarrier transmission system," in *2009 6th Inter. Sympos. Wireless Commun. Sys.*, pp. 206–210, Sept 2009.

[107] S. Trautmann and N. J. Fliege, "A new equalizer for multitone systems without guard time," *IEEE Commun. Lett.*, vol. 6, pp. 34–36, Jan 2002.

[108] C.-Y. Lin, J.-Y. Wu, and T.-S. Lee, "GSC-based frequency-domain equalizer for CP-free OFDM systems," in *IEEE Inter. Conf. Commun., ICC 2005.*, vol. 2, pp. 1132–1136 Vol. 2, May 2005.

[109] P. Wang, G. Yu, and Z. Zhang, "On the Secrecy Capacity of Fading Wireless Channel with Multiple Eavesdroppers," in *2007 IEEE Int. Symp. Inf. Theory*, pp. 1301–1305, IEEE, jun 2007.

[110] B. Xu, C. Yang, and S. Mao, "A multi-carrier detection algorithm for OFDM systems without guard time," in *ICC '03. IEEE Inter. Conf. Commun.*, vol. 5, pp. 3377–3381 vol.5, May 2003.

[111] S. Liu, M. Ma, Y. Li, Y. Chen, and B. Jiao, "An absolute secure wire-line communication method against wiretapper," *IEEE Commun. Lett.*, vol. 21, pp. 536–539, March 2017.

[112] A. Tom, A. Sahin, and H. Arslan, "Suppressing alignment: An approach for out-of-band interference reduction in OFDM systems," in *2015 IEEE Int. Conf. Commun.*, pp. 4630–4634, IEEE, jun 2015.

[113] Z. E. Ankaral, A. Sahin, and H. Arslan, "Joint time-frequency alignment for PAPR and OOBE suppression of OFDM-based waveforms," *IEEE Commun. Lett.*, vol. 21, pp. 2586–2589, Dec 2017.

[114] M. K. Ozdemir and H. Arslan, "Channel estimation for wireless OFDM systems," *IEEE Commun. Surv. Tut.*, vol. 9, pp. 18–48, Second 2007.

[115] G. Carlsson and V. de Silva, "A geometric framework for sparse matrix problems," *Advances in Applied Mathematics*, vol. 33, no. 1, pp. 1 – 25, 2004.

[116] M. Li, S. Kundu, D. A. Pados, and S. N. Batalama, "Securewaveforms for SISO channels," in *ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc.*, pp. 4713–4717, IEEE, may 2013.

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

[118] W. Y. Y. C. G. Yong Soo Cho, Jaekwon Kim, *MIMO-OFDM Wireless Communication with MATLAB*. Nov., 2010.

[119] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Trans. Commun.*, vol. 64, pp. 2578–2588, June 2016.

[120] A. Sahin, R. Yang, E. Bala, M. C. Beluri, and R. L. Olesen, "Flexible DFT-S-OFDM: Solutions and Challenges," *IEEE Commun. Mag.*, vol. 54, pp. 106–112, November 2016.

[121] Y. Rahmatallah and S. Mohan, "Peak-To-Average Power Ratio Reduction in OFDM Systems: A Survey And Taxonomy," *IEEE Commun. Surv. Tut.*, vol. 15, pp. 1567–1592, Fourth 2013.

[122] S. Shafiee and S. Ulukus, "Achievable Rates in Gaussian MISO Channels with Secrecy Constraints," in *Inf. Theory, 2007. ISIT 2007. IEEE Int. Symp.*, pp. 2466–2470, 2007.

[123] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.

[124] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-part II: The mimome wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[125] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, 2011.

[126] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the secrecy capacity of the wiretap channel with imperfect main channel estimation," *IEEE Trans. Commun.*, vol. 62, pp. 3652–3664, Oct 2014.

[127] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "Phy layer security based on protected zone and artificial noise," *IEEE Signal Process. Lett.*, vol. 20, pp. 487–490, May 2013.

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

[129] D. Kapetanović, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27r, 2015.

[130] T. Allen, J. Cheng, and N. Al-Dhahir, "Secure space-time block coding without transmitter CSI," *IEEE Wirel. Commun. Lett.*, vol. 3, pp. 573–576, Dec 2014.

[131] M. Nouri and A. Falahati, "Securing MIMO space-time block coding technique over wireless communication links," *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, 2012.

[132] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Sig. Process.*, vol. 59, no. 10, pp. 5013–5022, 2011.

[133] D. J. Love and R. W. Heath, "Limited feedback unitary precoding for orthogonal space-time block codes," *IEEE Transactions on Signal Processing*, vol. 53, pp. 64–73, Jan 2005.

[134] B. M. Hochwald, T. L. Marzetta, T. J. Richardson, W. Sweldens, and R. Urbanke, "Systematic design of unitary space-time constellations," *IEEE Trans. Info. Theory*, vol. 46, pp. 1962–1973, Sep 2000.

[135] M. H. Yilmaz, E. Guvenkaya, H. M. Furqan, S. Kose, and H. Arslan, "Cognitive security of wireless communication systems in the physical," *Wireless Commun. Mobile Comput.*, 2017.

[136] W. Trappe, "The challenges facing physical layer security.," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, 2015.

[137] P. Huang and X. Wang, "Fast secret key generation in static wireless networks: A virtual channel approach," in *2013 Proceedings IEEE INFOCOM*, pp. 2292–2300, April 2013.

[138] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang, "Smokegrenade: An efficient key generation protocol with artificial interference," *IEEE Trans. Info. Forensics Security*, vol. 8, pp. 1731–1745, Nov 2013.

[139] R. Guillaume, S. Ludwig, A. Mller, and A. Czylwik, "Secret key generation from static channels with untrusted relays," in *2015 IEEE 11th Inter. Conf. Wireless Mob. Comp. Netw. Commun. (WiMob)*, pp. 635–642, Oct 2015.

[140] S. Sharifian, F. Lin, and R. Safavi-Naini, "Secret key agreement using a virtual wiretap channel," in *IEEE INFOCOM 2017 - IEEE Conf. Computer Commun.*, pp. 1–9, May 2017.

[141] G. Li, A. Hu, J. Zhang, and B. Xiao, "Security analysis of a novel artificial randomness approach for fast key generation," in *GLOBECOM 2017 - 2017 IEEE Global Commun. Conf.*, pp. 1–6, Dec 2017.

[142] Y. Ding, J. Zhang, and V. F. Fusco, "Retrodirective-assisted secure wireless key establishment," *IEEE Trans. Commun.*, vol. 65, pp. 320–334, Jan 2017.

[143] P. Viswanath, D. N. C. Tse, and R. Laroia, "Opportunistic beamforming using dumb antennas," *IEEE Trans. Info. Theory*, vol. 48, pp. 1277–1294, Jun 2002.

[144] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *2011 Proceedings IEEE INFOCOM*, pp. 1125–1133, April 2011.

[145] T. Hong and Z. P. Li, "Peak-to-average power ratio reduction for an artificial noise aided secure communication system," in *2016 3rd Inter. Conf. Infor. Sci. Cont. Eng. (ICISCE)*, pp. 1370–1374, July 2016.

[146] J. M. Hamamreh and H. Arslan, "Joint PHY/MAC layer security design using ARQ with MRC and null-space independent, PAPR-aware artificial noise in SISO systems," *IEEE Trans. Wireless Commun.*, vol. To appear, 2018.

[147] J. Qiao, H. Zhang, X. Zhou, and D. Yuan, "Joint beamforming and time switching design for secrecy rate maximization in wireless-powered FD relay systems," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, pp. 1–1, 2017.

[148] A. Mostafa and L. Lampe, "Optimal and robust beamforming for secure transmission in MISO visible-light communication links," *IEEE Trans. Sig. Process.*, vol. 64, pp. 6501–6516, Dec 2016.

[149] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, 2013.

[150] M. Hafez, M. Yusuf, T. Khattab, T. Elfouly, and H. Arslan, "Secure spatial multiple access using directional modulation," *IEEE Trans. Wireless Commun.*, vol. 17, pp. 563–573, Jan 2018.

Appendix A

Appendix for Chapter 1

For the case of general L, which corresponds in practice to any type of delay-tolerant services such as web-browsing, chatting, FTP, etc., the generic formula of Eve's PER can be given as

$$\begin{aligned} PER_L^e(\bar{\gamma}_e, \bar{\gamma}_b, \alpha) &= \left(F_{\bar{\gamma}_e}^1(\alpha)\right) \times \left(1 - F_{\bar{\gamma}_b}^1(\alpha)\right) \\ &+ \sum_{v=1}^{L-2} \left(F_{\bar{\gamma}_e}^{v+1}(\alpha)\right) \times \left(F_{\bar{\gamma}_b}^{v}(\alpha)\right) \times \left(1 - F_{\bar{\gamma}_b}^{v+1}(\alpha)\right) \\ &+ \left(F_{\bar{\gamma}_e}^{L}(\alpha)\right) \times \left(F_{\bar{\gamma}_b}^{L-1}(\alpha)\right). \end{aligned} \tag{A.1}$$

After substituting the corresponding formulas of the CDFs into (41), Eve's PER becomes as

$$\begin{aligned} PER_L^e(\bar{\gamma}_e, \bar{\gamma}_b, \alpha) &= \left(1 - e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right) \times \left(e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right) \\ &+ \sum_{v=1}^{L-2} \left(1 - \sum_{m=0}^{v} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_e}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right) \\ &\times \left(1 - \sum_{m=0}^{v-1} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_b}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right) \\ &\times \left(\sum_{m=0}^{v} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_b}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right) \\ &+ \left(1 - \sum_{m=0}^{L-1} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_e}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right) \end{aligned}$$

$$\times \quad \left(1 - \sum_{m=0}^{L-2} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_b}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right). \tag{A.2}$$

Finally, by substituting PER_L^e given in (42) and PER_L^b given in (25) into (18), we can get a generic formula of the achievable secure throughput ($S\eta$) for any service with any L value. Note that the generic expression of Eve's PER given in (42) reduces to (29) when L=2, and to (32) when L=3.

ADVANCED CROSS-LAYER SECURE COMMUNICATION DESIGNS FOR FUTURE WIRELESS SYSTEMS

ORIGINALITY REPORT

12%	10%	5%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

< 1%

★ Submitted to University of South Florida

Student Paper

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		